IBM eMessage
Versão 8 Release 6
13 de fevereiro de 2015

Startup and Administrator's Guide

Índice

Capítulo 1. Sistema de mensagens hospedado usando o IBM Campaign e o IBM eMessage

Quando o IBM® Campaign estiver integrado com o IBM eMessage, você poderá usar o eMessage para conduzir campanhas de marketing altamente personalizadas por e-mail.

O eMessage fornece acesso a recursos hospedados pelo IBM para que você possa projetar, enviar e monitorar mensagens personalizadas individualmente com base nas informações armazenadas no datamart do cliente.

- No Campaign, use fluxogramas para criar listas de destinatários de e-mail e selecionar dados de personalização para cada destinatário.
- No eMessage, use recursos de projeto, transmissão e fornecimento de email hospedados pela IBM para conduzir campanhas de marketing por e-mail.

Estabelecendo uma conta de email hospedada com o IBM

Ao comprar uma assinatura do eMessage, o IBM cria uma conta de email hospedada em seu nome e envia as credenciais de conta que são necessárias para utilizar os recursos do eMessage. Aplique estas credenciais quando configurar seus aplicativos locais do IBM EMM para acessarem o ambiente de email hospedado sobre conexões seguras.

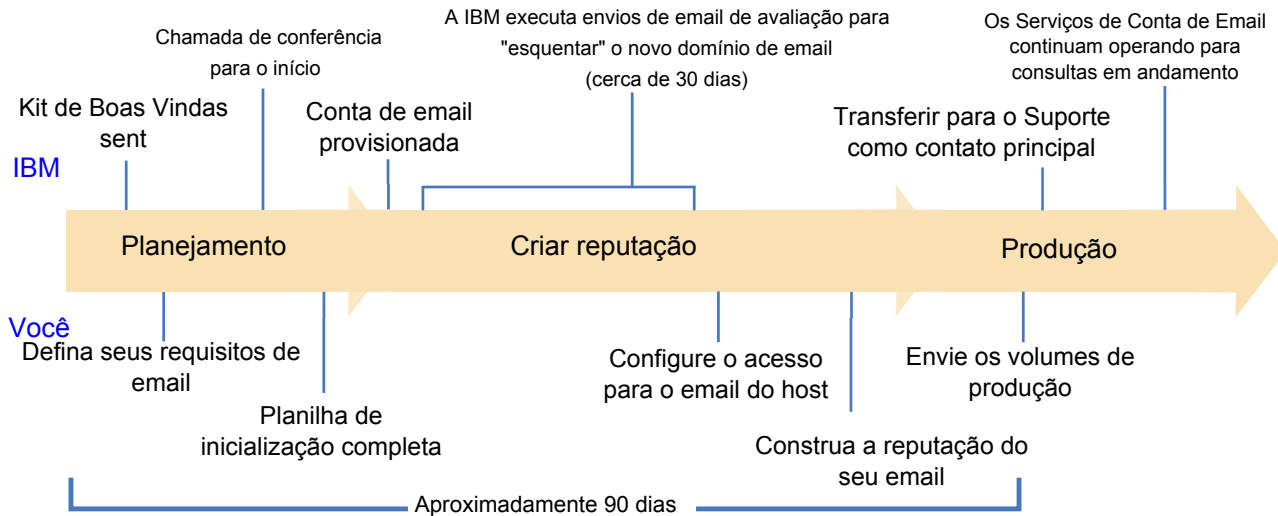
Deve-se ter uma conta válida para acessar os recursos de email que o IBM fornece como um serviço de software. Se a sua instalação do IBM EMM incluir várias partições e planejar usar o eMessage em mais de uma partição, uma conta de email hospedada será necessária para cada partição. Não é possível compartilhar as contas de email em instalações ou partições.

Estabelecer uma conta de email hospedada é o início do processo de inicialização que dura cerca de 90 dias. Para obter uma descrição geral do processo, consulte "Visão Geral do Processo de Inicialização".

Visão Geral do Processo de Inicialização

É possível ativar recursos de email no IBM Campaign para conduzir campanhas de marketing por email altamente direcionadas e rastreáveis. O Campaign usa as funções de email que são fornecidas pela IBM eMessage por meio de recursos que são hospedados em centros de dados nos Estados Unidos e Reino Unido. Uma conta para acessar esses recursos é incluída com a assinatura do eMessage.

O IBM inicia o processo de inicialização após criar sua conta de email hospedada. O IBM ajuda você a se familiarizar com o eMessage, se conectar aos recursos de email hospedados e estabelecer sua reputação como um legítimo comerciante por email entre os principais Provedores de Serviços da Internet (ISPs).

O processo continua em três fases. As equipes de Serviços de Conta de Email e Serviços Profissionais do IBM guiam você ao longo do caminho.

O consultor de Serviços Profissionais é o seu ponto de contato principal com o IBM durante o processo de inicialização. Quando o processo de inicialização da conta é concluído, o consultor de Serviços Profissionais transfere a responsabilidade do suporte primário para a equipe de Suporte de Produto do IBM .

Um consultor de Serviços de Conta de Email (EAS) dedicado fornece assistência especial para problemas relacionados a email. Criar uma reputação de email favorável entre os principais Provedores de Serviços da Internet (ISPs) é fundamental para assegurar que as suas campanhas de marketing de email atinjam de forma consistente seus destinatários alvos. Quando começar a executar correspondências, o consultor de EAS revisará o desempenho de fornecimento da correspondência e sugere as melhores maneiras para construir gradualmente a sua reputação de email.

Iniciando atividades e marcos

Planejando

O que acontece	Quem é responsável
Enviar as credenciais de conta de email e o Kit de Boas-vindas, incluindo a Planilha de Inicialização de Email.	Serviços de Conta de Email IBM
Planejar uma chamada de conferência para introduzir todas as partes envolvidas, revisar o planejamento de inicialização e entender os objetivos de marketing por email.	Serviços Profissionais do IBM
Preencha a Planilha de Inicialização de Email para especificar requisitos de domínio e projeções de correspondência para seu email.	Sua organização

Crie sua reputação de email

O que acontece	Quem é responsável
Prover a conta de email utilizando informações fornecidas durante a chamada de conferência e na planilha de Inicialização de Email.	Operações de email do IBM

O que acontece	Quem é responsável
Comece aquecendo as correspondências para contas de teste selecionadas com os principais ISPs. Esta fase requer aproximadamente 30 dias para ser concluída.	Operações de email do IBM
Ative o eMessage no IBM Campaign.	Sua organização (com suporte do IBM)
Configure o acesso aos recursos de email hospedado. Consulte um consultor de EAS sobre qual datacenter especificar.	Sua organização (com suporte do IBM)
Comece enviando correspondências. Para construir uma reputação de email favorável, envie correspondências inicialmente pequenas, seguido ao longo do tempo por correspondências maiores e mais frequentes. Os ISPs geralmente tentam limitar o spam ao bloquear correspondências grandes ou frequentes a partir de domínios de email que não forem reconhecidos como legítimos.	Sua organização (com suporte do IBM)
Forneça os resultados de fornecimento e orientação de reputação como volumes de correspondência e aumento gradual de frequência.	Serviços de Conta de Email IBM

Produção

O que acontece	Quem é responsável
Enviar correspondências em um volume e frequência típicos.	Sua organização
Transferir a responsabilidade do contato principal para a equipe de Suporte do IBM.	Serviços Profissionais do IBM
Manter compromisso para consulta sobre questões de email. Faça um contato regularmente para continuar com o suporte de conta de email.	Serviços de Conta de Email IBM

Antes de começar a trabalhar com o eMessage

Antes de iniciar o processo de inicialização de email hospedado, considere as seguintes questões.

- Algumas configurações requerem o reinício do servidor de aplicativos da web. Planeje a atividade de configuração do eMessage para evitar interferência com execuções de fluxogramas grandes e outras atividades no Campaign.
- O IBM solicita nomear um indivíduo para servir como o ponto de contato principal durante o processo de inicialização.
- Solicite credenciais de conta de email hospedada antes de começar o processo de inicialização. É possível utilizar essas credenciais para configurar seus sistemas para acessarem a conta.
- Consulte sua equipe de administração de rede. O eMessage requer intervalos de porta específicos quando se comunicar com o IBM EMM Hosted Services.
- Confirme se você tem as permissões de rede apropriadas para fazer mudanças na configuração.

Capítulo 2. Configurando o ambiente local do IBM EMM para o eMessage

Usar o eMessage para enviar mensagens de email hospedado requer mudanças na instalação local do IBM EMM. Conclua as etapas descritas nas seções a seguir.

- "Ativando Funções do eMessage no Campaign"
- "Registrar o eMessage manualmente, se necessário" na página 6
- "Especificando características de tabela de sistema do eMessage" na página 7
- "Mapeamento necessário para as tabelas de sistema do eMessage no Campaign" na página 9
- "Configurando o acesso às tabelas do sistema local do eMessage" na página 8
- "Reinicialização necessária do servidor de aplicativos da web para o Campaign" na página 9

Se o seu ambiente contiver diversas partições, repita estas etapas para cada partição do Campaign na qual é usado o IBM eMessage. Para obter mais informações sobre como criar e trabalhar com diversas partições, consulte o *Guia de Instalação do IBM Campaign*.

Ativando Funções do eMessage no Campaign

Ao instalar o Campaign, o instalador também instala o eMessage na partição padrão, mas não o ativa. As funções do eMessage não estão disponíveis até que ative o eMessage.

Antes de Iniciar

Confirme se o eMessage está registrado adequadamente com o IBM Marketing Platform.

Registrar o eMessage com o Marketing Platform é parte do processo de instalação para o IBM Campaign.

Procedimento

1. No IBM Marketing Platform, edite `Campanha > partições > partição[n] > servidor > interno > eMessageInstalled`.
2. Para ativar o eMessage, altere o valor para `yes`.

Tarefas relacionadas:

"Confirmando o registro do eMessage"

Confirmando o registro do eMessage

O IBM eMessage deve ser registrado com o IBM Marketing Platform. Para confirmar se o eMessage foi registrado com sucesso, deve-se examinar a configuração para Marketing Platform.

Procedimento

1. Efetue login noIBM EMM.
2. Navegue até **Configurações** > **Configuração**.
3. Procure a categoria de configuração do eMessage.

   O IBM eMessage é registrado com o Marketing Platform quando a categoria do eMessage aparece na hierarquia de propriedades de configuração.

O que Fazer Depois

Se a categoria do eMessage não aparecer na hierarquia de propriedades, consulte o *Guia de Instalação do IBM Campaign* para obter informações sobre como registrar o eMessage manualmente.

Se a categoria eMessage estiver disponível, você deve ativar as funções eMessage em Campaign.

Tarefas relacionadas:

"Ativando Funções do eMessage no Campaign" na página 5

Registrar o eMessage manualmente, se necessário

Se o instalador não registrar o eMessage automaticamente, você deverá registrar o eMessage manualmente com o utilitário `configTool` fornecido com a instalação do IBM EMM. O utilitário `configTool` está no diretório `tools\bin` em sua instalação do Marketing Platform.

Sobre Esta Tarefa

Por padrão, o instalador do Campaign registra automaticamente o eMessage com o IBM Marketing Platform, mas não o ativa. Em algumas situações, o instalador do Campaign não se conecta com as tabelas de sistema do Marketing Platform para registrar o eMessage automaticamente.

Para obter mais informações sobre o registro e configuração do eMessage, consulte o Guia de Inicialização e do Administrador do *IBM eMessage.*

Procedimento

Para registrar o eMessage manualmente, execute o utilitário `configTool` como a seguir.

```
configTool -r eMessage -f "full_path_to_eMessage_installation_directory\
conf\emessage_configuration.xml"
```

Nota: O diretório de instalação do eMessage é um subdiretório do diretório de instalação do Campaign.

Exibindo opções de menu do eMessage

Para usar o IBM eMessage, deve-se atualizar a configuração do sistema para que as opções de menu do eMessage sejam exibidas na interface do IBM Marketing Platform. Para exibir as opções necessárias, use o utilitário `configTool` que é fornecido com sua instalação do IBM EMM.

Deve-se executar o `configTool` com parâmetros específicos para cada opção de menu do eMessage. Executar `configTool` atualiza as definições de configuração do sistema. Deve-se reiniciar o servidor de aplicativos da web para aplicar as mudanças. Embora o eMessage seja instalado com o Campaign, as opções de menu do eMessage não aparecem até após executar `configTool` e reiniciar o servidor de aplicativos da web. No diretório `tools` da instalação do Marketing Platform, o utilitário `configTool` está localizado na pasta `bin`.

Nota: Deve-se especificar um caminho para o diretório de instalação do eMessage como um parâmetro `configTool`. O diretório de instalação do eMessage é um subdiretório do diretório de instalação do Campaign.

- Para exibir **Configurações do eMessage** no menu **Configurações**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|settingsMenu" -f
"full_path_to_eMessage_installation_directory\conf\
emessage_op_odsettings_navigation.xml"
```

- Para exibir **Correspondências do eMessage** no menu **Campanha**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Campaign"
-f "full_path_to_eMessage_installation_directory\conf\
emessage_op_mailings_navigation.xml"
```

- Para exibir **Documentos do eMessage** no menu do **Campaign**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Campaign"
-f "full_path_to_eMessage_installation_directory\conf\
emessage_op_documents_navigation.xml"
```

- Para exibir o **eMessage Analytics** no menu **Analytics**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Analytics"
-f "full_path_to_eMessage_installation_directory\conf\
emessage_op_analytics_navigation.xml"
```

Para verificar se as opções de menu foram incluídas com sucesso, após reiniciar o servidor de aplicativos da web, efetue login no IBM EMM e abra os menus **Configurações**, **Campaign** e **Analytics** para verificar se as opções do eMessage aparecem.

Especificando características de tabela de sistema do eMessage

O IBM eMessage requer informações que descrevem o tipo, esquema e conexão JDBC com as tabelas de sistema do eMessage em sua instalação. As tabela de sistema do eMessage são criadas no esquema do Campaign como parte do processo de instalação do Campaign.

Procedimento

Forneça as informações necessárias nas seguintes propriedades de configuração. Consulte a ajuda online do Marketing Platform para cada propriedade para saber mais sobre a definição das propriedades de configuração.

- `eMessage > partitions > partition [n] < dataSources > systemTables > type`
- `eMessage > partitions > partition [n] < dataSources > systemTables > schemaName`
- `eMessage > partitions > partition [n] < dataSources > systemTables > jdbcBatchSize`
- `eMessage > partitions > partition [n] < dataSources > systemTables > jdbcClassName`

- eMessage > partitions > partition [n] < dataSources > systemTables > jdbcURI

O que Fazer Depois

Para obter informações adicionais sobre as propriedades de configuração e configuração do eMessage, consulte Capítulo 6, "Configurações para o IBM eMessage", na página 41.

Configurando o acesso às tabelas de sistema do eMessage

Os componentes do eMessage devem ser capazes de acessar as tabelas de sistema automaticamente, sem entrada manual do usuário. Para permitir que os componentes do eMessage acessem as tabelas de sistema no esquema do Campaign sem solicitar um login de banco de dados manual, defina um usuário do sistema no IBM Marketing Platform. Deve-se configurar esse usuário do sistema para fornecer as credenciais de acesso para o banco de dados que contém o esquema do Campaign.

Configure os usuários do sistema e as origens de dados no IBM Marketing Platform. Para obter mais informações sobre como criar usuários do sistema e origens de dados, consulte o *Guia do Administrador do IBM Marketing Platform*.

Configurando o acesso às tabelas do sistema local do eMessage

O IBM eMessage requer acesso às tabelas de sistema do eMessage no esquema do Campaign. Para permitir que os componentes eMessage acessem as tabelas do sistema no esquema Campaign sem solicitar um login de banco de dados manual, deve-se especificar um usuário do sistema eMessage para fornecer as credenciais necessárias de acesso ao banco de dados.

Sobre Esta Tarefa

O usuário do sistema que acessa o banco de dados está associado a uma origem de dados IBM Marketing Platform que contém as credenciais de login para o banco de dados que hospeda o esquema do Campaign.

Para obter informações adicionais sobre as propriedades de configuração de tabela de sistema, consulte "eMessage | Partições | Partição[n] | dataSources | systemTables" na página 52.

Procedimento

1. Especifique o usuário do sistema que você definiu no IBM Marketing Platform. Edite a propriedade de configuração a seguir.

   eMessage > partitions > partition [n] < dataSources > systemTables > asmUserForDBCredentials
2. Especifique as credenciais de login para o banco de dados que contém o esquema Campaign e as tabelas do sistema eMessage. Edite a propriedade de configuração a seguir.

   eMessage > partitions > partition [n] < dataSources > systemTables > amDataSourceForDBCredentials

Mapeamento necessário para as tabelas de sistema do eMessage no Campaign

Deve-se mapear as tabelas de sistema do eMessage no esquema do Campaign para as tabelas de banco de dados correspondentes do eMessage As tabelas de sistema do eMessage têm o **eMessage** no nome da tabela.

No Campaign, mapeie as seguintes tabelas de sistema do eMessage .

- Tabela da lista de saída eMessage
- Tabela de Mapeamento de Campos de Público de Lista de Saída do eMessage
- Tabela de Correspondências do eMessage
- Tabela de Instâncias de Correspondências do eMessage
- Tabela de Mapeamento de Colunas da Tabela de Dados do eMessage
- Tabela de Mapeamento de Campo de Personalização do eMessage
- Tabela de Uso do Campo de Personalização do eMessage

Para obter informações sobre o mapeamento de tabelas, consulte o *IBM Campaign Administrator's Guide*.

Reinicialização necessária do servidor de aplicativos da web para o Campaign

Após fazer as mudanças nas configurações do Campaign e do eMessage, deve-se reiniciar o servidor de aplicativos da web que hospeda o Campaign.

Consulte a documentação para o seu servidor de aplicativos da web para instruções de como reiniciar.

Capítulo 3. Conexões aos serviços de email hospedados

Para acessar os serviços de email hospedados fornecidos pelo IBM, você deve configurar uma conexão entre a instalação local do IBM EMM e do IBM EMM Hosted Services.

Os comerciantes acessam os recursos do eMessage por meio da interface do Campaign. Trabalhar com o eMessage requer que você estabeleça uma conexão com a Internet segura e automática que o Campaign pode utilizar para fazer upload de listas de destinatários de email do IBM EMM Hosted Services. Os componentes instalados com o eMessage Campaign também utilizam esta conexão para fazer download de dados de contato e de resposta para as tabelas de sistema do eMessage no esquema do Campaign.

Nota: Cada instância do Campaign requer uma conexão exclusiva com o IBM EMM Hosted Services. Se a instalação do Campaign incluir diversas partições, cada uma delas requer uma conta de email hospedada separada. As contas podem compartilhar a conexão IP com o IBM EMM Hosted Services.

Toda a comunicação entre o IBM EMM e o IBM EMM Hosted Services é feita por meio de SSL. Cada comunicação a partir do IBM EMM Hosted Services é uma resposta a uma solicitação do ambiente local. O IBM EMM Hosted Services nunca tenta iniciar uma conexão com sua rede corporativa. Toda a comunicação com o IBM EMM Hosted Services é originada atrás de seu firewall corporativo.

Requisitos para configurar a conexão com o IBM EMM Hosted Services

Configurar uma conexão com o IBM EMM Hosted Services requer permissões administrativas e informações sobre a conta de email hospedada estabelecida para sua organização.

Para configurar uma conexão de email hospedado, é necessário o seguinte.

- Nome do usuário e a senha fornecidos pelo IBM para a conta de email hospedada
- As permissões para criar ou modificar os usuários do sistema no IBM Marketing Platform
- O acesso administrativo para as propriedades de configuração mantidas na instalação local do IBM Marketing Platform.
- Acesso administrativo ao servidor de aplicativos da web no qual o IBM Marketing Platform e o Campaign estão implementados

Deve-se saber ou ser capaz de consultar pessoas que conhecem os requisitos de segurança de dados corporativos. Antes de iniciar, revise estes procedimentos para entender como criar a conexão necessária em conformidade com suas restrições de firewall corporativo.

Deve-se estar familiarizado com o modo de configuração de conexões confiáveis no servidor de aplicativos da web, o IBM WebSphere ou Oracle WebLogic.

Requisitos para fazer upload dos dados para IBM EMM Hosted Services

Um componente do eMessage chamado Recipient List Uploader (RLU) faz parte de sua instalação do IBM Campaign. O RLU usa o FTP no modo passivo para gerenciar o upload de listas de distribuições de email e metadados associados ao IBM EMM Hosted Services.

O eMessage usa FTP passivo para fazer upload de dados. Ao utilizar o FTP passivo, o RLU inicia todas as solicitações de conexão de upload como o cliente local. O IBM EMM Hosted Services nunca inicia uma solicitação de conexão com sua rede.

O eMessage suporta dois métodos de FTP passivos, o FTP explícito e o FTP implícito. O FTP explícito é o método padrão utilizado para fazer upload de listas de destinatários. Para usar o FTP implícito, deve-se fazer mudanças nas propriedades de configuração do eMessage.

Para obter mais informações sobre o FTP no modo passivo e utilizar FTP sobre SSL, consulte RFC959 e RFC2228.

Conceitos relacionados:

"Conexão de upload padrão por meio de FTP explícito" na página 13

"Fazendo upload de dados com FTP implícito" na página 14

Requisitos de conexão e de porta

Para se comunicar com o IBM EMM Hosted Services, deve-se possuir uma conexão com a Internet. O IBM EMM Hosted Services usa portas específicas.

A instalação local do IBM EMM e do IBM EMM Hosted Services utiliza as seguintes portas para se comunicar.

HTTPS: porta 443

Porta do comando FTP:

- FTP explícito: porta 21
- FTP implícito: porta 990

Portas de upload de dados de FTP

- datacenter dos EUA

  FTP explícito: portas 15393 a 15424

  FTP implícito: portas 15600 a 15701
- Datacenter do Reino Unido

  FTP explícito: porta 15393 a 15443

  FTP implícito: portas 15600 a 15650

O IBM EMM Hosted Services nunca inicia uma conexão com sua rede local. Ele apenas responde às solicitações de conexão iniciadas a partir de trás do firewall.

Conexão de upload padrão por meio de FTP explícito

Por padrão, o Recipient List Uploader (RLU) utiliza FTP explícito quando o sistema faz upload de uma lista de destinatários de email. A lista de destinatários é também referenciada como a Tabela de Lista de Saída (OLT)

O RLU estabelece uma conexão com o IBM EMM Hosted Services por meio da porta de comando FTP padrão (porta 21). Ele emite uma solicitação para criptografar a sessão sobre SSL. Durante a conexão segura, o RLU negocia com o servidor FTP para estabelecer um link SSL separado por meio de uma porta que é selecionada aleatoriamente pelo RLU. Para obter mais informações sobre FTP explícito, consulte o RFC 2228.

O diagrama a seguir ilustra o método padrão para fazer upload de dados de destinatários a partir do Campaign para o IBM EMM Hosted Services.

A tabela a seguir descreve a sequência da conexão.

Etapa	Ação	Descrição
1	Solicitação de conexão inicial do cliente FTP	Por trás do firewall corporativo, o RLU inicia uma sessão de upload de dados utilizando o FTP sobre SSL explícito. O RLU envia a solicitação de conexão SSL para o endereço do IBM EMM Hosted Services. Deve-se configurar esse endereço com antecedência. Para iniciar a sessão, o RLU abre uma porta selecionada aleatoriamente no lado do cliente como sua porta de comandos FTP. O IBM EMM Hosted Services aceita conexões do comando FTP na porta 21.
2	Resposta do servidor de FTP remoto	Em resposta à solicitação do RLU uma sessão SSL segura, o servidor FTP designa a porta de dados de FTP a ser utilizada para o upload da lista de destinatários.

Etapa	Ação	Descrição
3	Upload da Lista de Destinatários	O RLU inicia o upload da lista na porta de dados especificada. Quando o upload for concluído, o RLU eliminará a conexão de FTP.

Para obter o intervalo de dados de portas que o servidor FTP pode especificar, consulte "Requisitos de conexão e de porta" na página 12.

Conceitos relacionados:

"Requisitos para fazer upload dos dados para IBM EMM Hosted Services" na página 12

Tarefas relacionadas:

"Configurando endereços para conectar ao IBM EMM Hosted Services" na página 25

"Configurando o usuário do sistema que acessa o IBM EMM Hosted Services" na página 23

Configurando a conexão de FTP explícita

Nenhuma configuração adicional é exigida. O RLU utiliza FTP explícito por padrão.

Fazendo upload de dados com FTP implícito

É possível configurar o RLU para usar FTP implícito para fazer upload de listas de destinatários de email. O FTP implícito utiliza a porta 990 para estabelecer uma conexão com o IBM EMM Hosted Services.

Ao ativar o RLU para FTP implícito, a sessão inteira é criptografada desde o início. O FTP implícito é uma conexão diferente do FTP explícito porque o RLU solicita explicitamente um link seguro.

Para utilizar o FTP implícito para fazer upload de listas de destinatários, deve-se revelar e configurar uma propriedade de configuração do sistema nas propriedades de configuração do eMessage.

O diagrama a seguir ilustra como o RLU faz uploads de dados do destinatário para o IBM EMM Hosted Services quando o sistema é configurado para usar FTP implícito.

A tabela a seguir descreve a sequência da conexão.

Etapa	Ação	Descrição
1	Solicitação de conexão inicial do cliente FTP	Por trás do firewall corporativo, o RLU inicia uma sessão de upload de dados utilizando o FTP sobre SSL. O RLU envia a solicitação de conexão SSL para o endereço do IBM EMM Hosted Services. Deve-se configurar esse endereço com antecedência. Para iniciar a sessão, o RLU abre a porta 990. O IBM EMM Hosted Services aceita conexões de comando FTP criptografadas apenas na porta 990.
2	Resposta do servidor de FTP remoto	Se o IBM EMM Hosted Services reconhecer a solicitação como uma solicitação de FTP implícito válida, o servidor FTP aceitará essa solicitação de conexão. Ele designa a porta de dados de FTP a ser utilizada para o upload da lista de destinatários. Consulte o “Requisitos de conexão e de porta” na página 12 para o intervalo de porta de dados que o servidor FTP pode especificar.
3	Upload da Lista de Destinatários	O RLU inicia o upload da lista na porta de dados especificada. Quando o upload for concluído, o RLU eliminará a conexão de FTP.

Conceitos relacionados:

“Requisitos para fazer upload dos dados para IBM EMM Hosted Services” na página 12

Acessando os parâmetros de configuração para upload de FTP implícito

Para configurar o sistema para usar o FTP implícito para fazer upload dos dados, você deve editar as propriedades de configuração ocultas por padrão. Execute um script para revelar as propriedades.

Sobre Esta Tarefa

Para configurar o sistema para usar o FTP implícito para fazer upload dos dados, torne as propriedades de configuração a seguir visíveis. Essas propriedades estão ocultas por padrão.

- `eMessage > serverComponentsAndLocations > hostedServices > ftpPort`
- `eMessage > serverComponentsAndLocations > hostedServices > useFTPImplicitSSL`

Este procedimento exibe as propriedades de configuração, mas não a configura. Para ativar o FTP implícito, deve-se acessar estas propriedades na configuração do eMessage e configurá-las. Para obter informações sobre como configurar essas propriedades, consulte "Ativando upload de FTP implícito".

Procedimento

Para revelar `ftpPort` e `useFTPImplicitSSL`, no diretório **Ferramentas** de sua instalação do eMessage, execute o script `switch_config_visibility` a partir do script da linha de comandos, como a seguir.

Windows

```
\switch_config_visibility.bat -p
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|ftpPort" -v
true
\switch_config_visibility.bat -p
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|
useFTPImplicitSSL" -v true
```

UNIX

```
/switch_config_visibility.sh
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|ftpPort" -v
true
/switch_config_visibility.sh
"Affinium|eMessage|serverComponentsAndLocations|hostedServices|
useFTPImplicitSSL" -v true
```

O que Fazer Depois

Deve-se reiniciar o servidor de aplicativos da web para tornar estas propriedades visíveis na configuração do eMessage.

Tarefas relacionadas:

"Configurando o acesso ao histórico de execução da correspondência adicional" na página 43

Ativando upload de FTP implícito

Para ativar o FTP implícito, deve-se atualizar a configuração do eMessage.

Antes de Iniciar

Para concluir esta tarefa, deve-se revelar duas propriedades de configuração. Para obter informações adicionais, consulte o “Acessando os parâmetros de configuração para upload de FTP implícito” na página 16.

Procedimento

1. Navegue para `Configurações > Configuração > eMessage > serverComponentsAndLocations > hostedServices`.
2. Clicar em **Editar Configurações**.
   - Confirme se `useFTPImplicitSSL` foi configurado para `true`.
   - Configure `ftpPort` para `990`.
3. Salve suas mudanças.

O que Fazer Depois

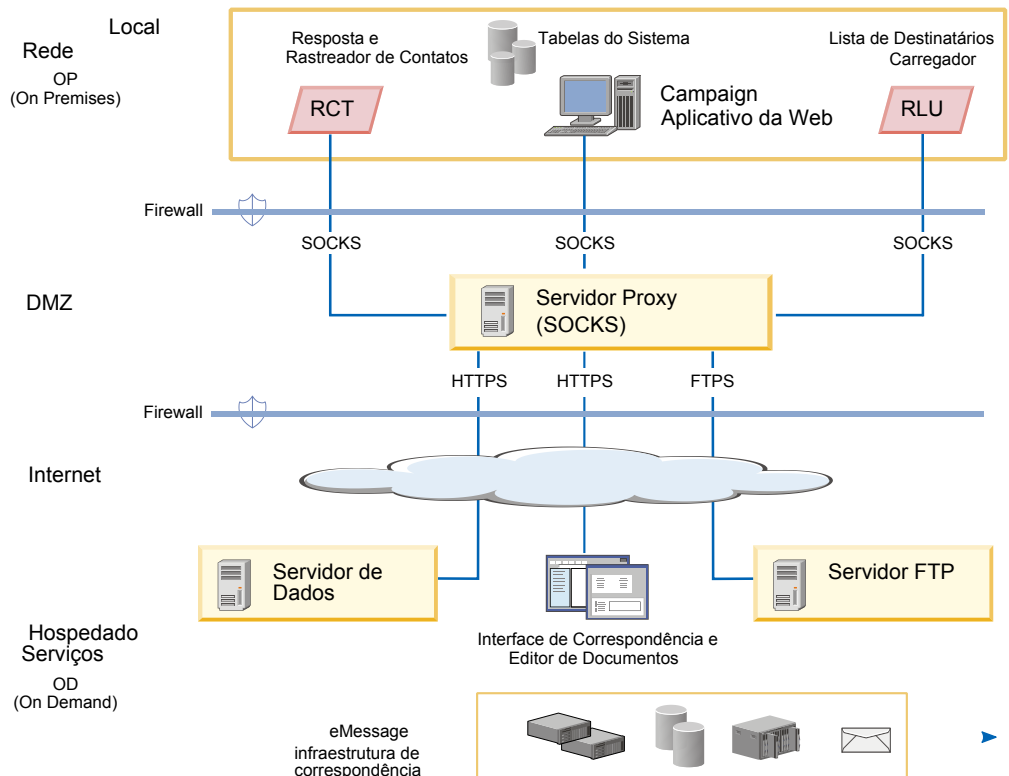
As mudanças não entram em vigor até reiniciar o servidor de aplicativos da web e o listener do Campaign. É possível fazer isso agora ou aguardar até que todas as etapas de configuração de inicialização sejam concluídas.

Conexão por meio de um proxy HTTP

Se a suas regras de firewall corporativas proibirem a comunicação direta com a Internet pública, será possível se conectar com o IBM EMM Hosted Services por meio de um servidor proxy HTTP. O eMessage suporta a conexão por meio de um servidor proxy SOCKS que permite tráfego tanto HTTPS quanto FTPS.

O eMessage suporta o SOCKS Protocol Versão 5.

Nota: Para conectar-se ao IBM EMM Hosted Services por meio de um servidor proxy, deve-se instalar o Campaign versão 8.5.0.1 ou superior.

O diagrama a seguir ilustra a comunicação entre os ambientes local e hospedados ao usar um proxy SOCKS.

Configure o servidor proxy SOCKS no ambiente On Premises local. Antes de começar a configurar o servidor proxy, confirme se os seguintes requisitos foram satisfeitos.

- O servidor proxy deve ser um servidor proxy SOCKS.
- O servidor proxy deve ser capaz de acessar o ambiente eMessage OD. O servidor deve permitir o tráfego para e a partir das portas que são configuradas para o datacenter que é utilizado por sua conta de email hospedada. O IBM mantém os datacenters nos Estados Unidos e no Reino Unido.
- O ambiente eMessage OP deve ser capaz de acessar o servidor proxy SOCKS.

Configurando o roteamento para tráfego FTPS e HTTPS por meio de um proxy SOCKS

Para utilizar um proxy SOCKS para acessar os recursos de email hospedado, deve-se atualizar o servidor de aplicativos da web no qual implementou o IBM Campaign. Também se deve modificar os scripts de inicialização para o RCT ou RLU do eMessage.

Procedimento

- Para o tráfego FTPS, aplique as configurações a seguir para o RLU e o servidor de aplicativos da web.

Configuração	Descrição
`-Dibm.unica.emessage.ftps.proxy.host = <socksHost>`	Nome do host ou IP do proxy SOCKS.
`-Dibm.unica.emessage.ftps.proxy.port = <socksPort>`	A porta na qual o proxy SOCKS está em execução.

Configuração	Descrição
-Dibm.unica.emessage.ftps.proxy.match.hosts= <lista separada por vírgula de nomes do host e endereços IP>	Os nomes de host e endereços IP que são utilizados ao rotear o tráfego por meio do proxy SOCKS. Forneça valores específicos para o datacenter utilizado pela sua conta.

Quando ambientes locais e hospedados estabelecem uma conexão de dados, o endereço IP que é especificado para -Dibm.unica.emessage.ftps.proxy.match.hosts é o endereço IP que o servidor FTP remoto envia ao cliente FTP local.

Configure -Dibm.unica.emessage.ftps.proxy.match.hosts para um dos seguintes valores. O valor que você insere depende do datacenter que é utilizado pela sua conta de email hospedada.

O nome do host e endereços IP para o datacenter dos Estados Unidos:

```
-Dibm.unica.emessage.ftps.proxy.match.hosts=

ftp-
em.unicaondemand.com,192.86.44.132,192.86.44.133,192.86.44.134,192.86.45.132,192.86.45.133,192.86.45.134
```

Nome do host e endereços IP para o datacenter do Reino Unido:

```
-Dibm.unica.emessage.ftps.proxy.match.hosts=

ftp-em-
eu.unicaondemand.com,192.86.45.132,192.86.45.133,192.86.45.134,192.86.44.132,192.86.44.133,192.86.44.134
```

- Para o tráfego HTTPS, aplique as configurações a seguir para o RCT e o servidor de aplicativos da web.

Configuração	Descrição
-Dibm.unica.emessage.https.proxy.host=<socksHost>	Nome do host ou IP do proxy SOCKS
-Dibm.unica.emessage.https.proxy.port=<socksPort>	A porta na qual o proxy SOCKS está em execução
-Dibm.unica.emessage.https.proxy.type=SOCKS	O tipo de servidor proxy. Deve-se utilizar um servidor proxy SOCKS.

Configurando a autenticação para acessar um proxy SOCKS

Se o proxy SOCKS requerer autenticação, deve-se configurar o servidor de aplicativos da web, o RLU e o RCT para fornecerem as credenciais de acesso.

Procedimento

Configure o seguinte para o servidor de aplicativos da Web, RLU e RCT. Os valores para username e password devem ser as credenciais que são necessárias para autenticar-se no proxy.

```
-Dibm.unica.emessage.proxy.auth.user = <username>
-Dibm.unica.emessage.proxy.auth.password = <password>
```

Configurando o RCT para utilizar um proxy SOCKS

Deve-se modificar o RCT para se comunicar por meio de um servidor proxy SOCKS. As configurações necessárias dependem de seu sistema operacional.

Procedimento

- Para o RCT em ambientes Windows, inclua os argumentos proxy a seguir no `common.bat`. O arquivo `common.bat` está no diretório `//eMessage/bin` de sua instalação local do eMessage.

```
set RCT_PROXY_ARGS=

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>

set RCT_JAVA_ARGS=%BASE_VM_ARGS% %RCT_MEM_ARGS%

%RCT_EXTRA_VM_ARGS% %RCT_PROXY_ARGS%
```

- Para o RCT em ambientes UNIX, inclua os argumentos proxy a seguir no `common.sh`. O arquivo `common.sh` está no diretório `\\eMessage\bin` de sua instalação local do eMessage .

  Nota: Não modifique diretamente o `rlu.sh`, `rct.sh` ou `setenv.sh`. O sistema substitui as mudanças.

```
RCT_PROXY_ARGS="

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>"

RCT_JAVA_ARGS="${BASE_VM_ARGS} ${RCT_MEM_ARGS} ${RCT_EXTRA_VM_ARGS}
${RCT_PROXY_ARGS}"
```

Configurando o RLU para utilizar um proxy SOCKS

Deve-se modificar o RLU para se comunicar por meio de um servidor proxy SOCKS. As configurações necessárias dependem de seu sistema operacional.

Procedimento

- Para o RLU em ambientes Windows, inclua os argumentos proxy a seguir no `common.bat.` O arquivo `common.bat` está no diretório `//eMessage/bin` de sua instalação local do eMessage.

```
set RLU_PROXY_ARGS=

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<comma separated list of host names
and IP addresses>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>

set RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_ARGS%

%RLU_PROXY_ARGS%
```

- Para o RLU em ambientes UNIX, inclua os argumentos proxy a seguir no `common.sh`. O arquivo `common.sh` está no diretório `\\eMessage\bin` de sua instalação local do eMessage .

  Nota: Não modifique diretamente o `rlu.sh`, `rct.sh` ou `setenv.sh`. O sistema substitui as mudanças.

```
RLU_PROXY_ARGS="

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<comma separated list of host names
and IP addresses>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>"

RLU_JAVA_ARGS="${BASE_JAVA_ARGS} ${RLU_MEM_ARGS} ${RLU_EXTRA_VM_ARGS}

${RLU_PROXY_ARGS}"
```

Configurando o servidor de aplicativos da web para usar um proxy SOCKS

Para conectar-se ao IBM EMM Hosted Services por meio de um proxy SOCKS, deve-se modificar a configuração do servidor de aplicativos da web. Para o servidores do IBM WebSphere, modifique os argumentos genéricos da JVM. Para servidores Oracle Weblogic, modifique o script `SetDomainEnv`.

Procedimento

- Se o seu servidor de aplicativos da web for o IBM WebSphere, inclua o seguinte nos argumentos genéricos da JVM do WebSphere.

```
-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<comma separated list of host names
and IP addresses>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>
```

- Se o seu servidor de aplicativos da web for o Oracle WebLogic, modifique o script `setDomainEnv`. As configurações necessárias dependem de seu sistema operacional.

  Em ambientes Windows, faça as seguintes mudanças:

```
JAVA_OPTIONS =%{JAVA_OPTIONS}

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<comma separated list of host names
and IP addresses>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>
```

  Em ambientes UNIX, faça as seguintes mudanças:

```
JAVA_OPTIONS ='${JAVA_OPTIONS}

-Dibm.unica.emessage.https.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.https.proxy.port=<PROXY_PORT>

-Dibm.unica.emessage.https.proxy.type=SOCKS

-Dibm.unica.emessage.ftps.proxy.host=<PROXY_HOST>

-Dibm.unica.emessage.ftps.proxy.port=<POXY_PORT>

-Dibm.unica.emessage.ftps.proxy.match.hosts=<comma separated list of host names
and IP addresses>

-Dibm.unica.emessage.proxy.auth.user=<PROXY_AUTH_USER>

-Dibm.unica.emessage.proxy.auth.password=<PROXY_AUTH_PASSWORD>'
```

Frequência de download de dados e configuração de porta

Um componente eMessage denominado Response and Contact Tracker (RCT) é instalado como parte de sua instalação do IBM Campaign. O RCT solicita regularmente resposta de email e dados de rastreamento do IBM EMM Hosted Services. Por padrão, o RCT emite uma solicitação de dados a cada 5 segundos.

O RCT emite solicitações de dados por meio de HTTPS (HTTP sobre SSL). O IBM EMM Hosted Services aceita solicitações de conexão HTTPS na porta 443 e apenas de hosts que você especificou durante o processo de inicialização de conta de email hospedada.

Conceitos relacionados:

Capítulo 4, "Operação Response and Contact Tracker", na página 33

Usuário do sistema para acessar o IBM EMM Hosted Services

Os componentes do IBM eMessage devem ser capazes de se comunicar com o IBM EMM Hosted Services sem requerer entrada manual de credenciais de login. Para estabelecer login automático, defina um usuário do sistema no IBM Marketing Platform que possa fornecer as credenciais de acesso necessárias.

Para simplificar a administração e a resolução de problemas do usuário, é possível modificar um usuário do sistema existente para acessar os serviços e tabelas de sistema locais hospedados. É possível configurar um único usuário do sistema para fornecer credenciais para diversos sistemas. Por exemplo, modificar a configuração do usuário do sistema do Campaign cria um único usuário que pode acessar automaticamente as tabelas do sistema do IBM EMM Hosted Services e do eMessage no esquema do Campaign.

As credenciais necessárias para acessar o IBM EMM Hosted Services são o nome de usuário e senha que a IBM forneceu durante o processo de inicialização. As credenciais que você usa dependem se você está se conectando ao datacenter que o IBM mantém nos EUA ou ao datacenter no Reino Unido. Consulte o IBM para determinar qual datacenter será usado.

Para obter informações específicas sobre como configurar um usuário do sistema para se comunicar com o IBM EMM Hosted Services, consulte o *IBM Guia do Administrador e de Inicialização do eMessage*.

Para obter informações gerais sobre como criar usuários do sistema e origens de dados, consulte o *Guia do Administrador do IBM Marketing Platform*.

Configurando o usuário do sistema que acessa o IBM EMM Hosted Services

Os componentes do eMessage no Campaign devem ser capazes de acessar o IBM EMM Hosted Services automaticamente, sem solicitar um login. Os usuários do sistema que estão configurados no IBM Marketing Platform podem referenciar uma origem de dados que forneça o nome do usuário e a senha necessários. É possível incluir a origem de dados em um novo usuário do sistema ou em um usuário do sistema existente. Para simplificar a administração de usuário, é possível atualizar um usuário do sistema que já esteja configurado para acessar o esquema do Campaign para que possa acessar também o IBM EMM Hosted Services.

Antes de Iniciar

Para concluir esta tarefa, você deve saber o nome de usuário e senha do IBM EMM Hosted Services que o IBM designou para a conta de email hospedada. Receber o nome do usuário e a senha faz parte do processo de inicialização da conta.

Deve-se ter as permissões de acesso apropriadas e saber como criar usuários do sistema e origens de dados no IBM Marketing Platform.

Sobre Esta Tarefa

Nota: Se a sua instalação contiver várias partições, deve-se concluir esta tarefa para cada partição. Não é possível compartilhar usuários do sistema nas partições.

Procedimento

1. Crie uma origem de dados da plataforma para conter o nome de usuário e a senha que são necessários para acessar o IBM EMM Hosted Services. Para obter melhores resultados e facilitar a manutenção, nomeie esta origem de dados como UNICA_HOSTED_SERVICES. Configure esta origem de dados como a seguir.

   Para **Login da Origem de Dados**, digite o nome do usuário que você recebeu do IBM durante a inicialização da conta.

   Para **Senha da Origem de Dados**, digite a senha que recebeu IBM durante a inicialização da conta.
2. Especifique a origem de dados na configuração do eMessage. Utilize a propriedade de configuração do **`amDataSourceForAcctCredentials`**.

   A propriedade de configuração está em `eMessage > partitions > partition[n] > hostedAccountInfo >` **`amDataSourceForAcctCredentials`**.

   Por padrão, a origem de dados especificada é `UNICA_HOSTED_SERVICES`.
3. Especifique um usuário do sistema para acessar o IBM EMM Hosted Services. É possível especificar um usuário existente ou criar um usuário. Na configuração do eMessage, utilize a propriedade de configuração **`amUserForAcctCredentials`**.

   A propriedade de configuração está em `eMessage > partitions > partition[n] > hostedAccountInfo >` **`amUserForAcctCredentials`**.

   Por padrão, o usuário especificado é `asm_admin`.
4. Inclua a origem de dados que é configurada na Etapa 1 para o usuário do sistema especificado na Etapa 3.

O que Fazer Depois

Deve-se reiniciar o servidor de aplicativos da web para que as mudanças na configuração entrem em vigor.

Conceitos relacionados:

"Conexão de upload padrão por meio de FTP explícito" na página 13

"Confirmação para configurações do sistema" na página 37

Configurando os endereços utilizados para se conectar ao IBM EMM Hosted Services

Para assegurar a conexão correta com o IBM EMM Hosted Services, deve-se inserir os endereços como valores para as propriedades de configuração na configuração do eMessage. Os endereços de conexão que você insere dependem de você estar se conectando ao datacenter do IBM dos EUA ou ao datacenter do IBM no Reino Unido.

Consulte o IBM para confirmar qual datacenter sua conta de email hospedada utiliza.

Para obter mais informações sobre como configurar informações de conexão, consulte "Configurando endereços para conectar ao IBM EMM Hosted Services".

Configurando endereços para conectar ao IBM EMM Hosted Services

Para assegurar a conexão correta com o IBM EMM Hosted Services, deve-se inserir os endereços como valores para as propriedades de configuração na configuração do eMessage. Os endereços de conexão que você insere dependem de você estar se conectando ao datacenter do IBM dos EUA ou ao datacenter do IBM no Reino Unido.

Antes de Iniciar

Consulte o IBM para confirmar qual datacenter sua conta de email hospedada utiliza.

Procedimento

No IBM Marketing Platform, navegue para **Configurações > Configuração**. Na configuração do eMessage, navegue para as seguintes propriedades de configuração do eMessage e confirme ou atualize as configurações de conexão, dependendo de seu datacenter que a sua conta utiliza.
Use as configurações padrão, se sua conta se conectar ao datacenter dos EUA.

- `eMessage > serverComponentsAndLocations > hostedServices> uiHostName`

  O padrão é `em.unicaondemand.com`.

  Para conectar-se ao datacenter do IBM no Reino Unido, altere este valor para `em-eu.unicaondemand.com`.
- `eMessage > serverComponentsAndLocations > hostedServices> dataHostName`

  O padrão é `em.unicaondemand.com`.

  Para conectar-se ao datacenter do IBM no Reino Unido, altere este valor para `em-eu.unicaondemand.com`.
- `eMessage > serverComponentsAndLocations > hostedServices> ftpHostName`

  O padrão é `ftp-em.unicaondemand.com`.

  Para conectar-se ao datacenter do IBM no Reino Unido, altere este valor para `ftp-em-eu.unicaondemand.com`.

O que Fazer Depois

Se alterar uma propriedade de configuração, reinicie o servidor de aplicativos da web para aplicar as mudanças.

Conceitos relacionados:

"Conexão de upload padrão por meio de FTP explícito" na página 13

Configurando comunicação segura para email hospedado

A comunicação entre o comerciante por email e o IBM EMM Hosted Services ocorre sobre Secure Sockets Layer (SSL). Deve-se alterar a configuração do servidor de aplicativos da web para utilizar SSL. Fazer as mudanças necessárias requer o uso do utilitário Java™ `keytool`.

Configurar a comunicação segura envolve as seguintes ações.

- Gerar um keystore confiável.
- Obter um certificado digital a partir do IBM EMM Hosted Services.
- Incluir o keystore confiável no servidor de aplicativos da web.
- Importar o certificado digital do IBM EMM Hosted Services no keystore confiável.

As etapas e a sequência exatas necessárias para configurar o SSL dependem do tipo e da versão do servidor de aplicativos da web (WebSphere ou WebLogic) no qual você implementou o IBM Marketing Platform e o IBM Campaign.

Para o WebLogic, consulte "Configurando SSL ao utilizar o WebLogic" na página 28.

Para o WebSphere, consulte "Configurando o SSL quando usar o IBM WebSphere" na página 30.

Gerando um keystore confiável

Siga este procedimento para criar um keystore de identidade e um keystore confiável para configurar o IBM eMessage para se comunicar com o IBM EMM Hosted Services por meio de SSL. Inclua os keystores no servidor de aplicativos da web quando configurar o SSL.

Sobre Esta Tarefa

A IBM utiliza os valores de amostra a seguir nos procedimentos contidos nesta seção.

- Keystore de identidade: `IBMUnicaClientIdentity.jks`
- Alias para o keystore de identidade: `IBMUnicaClientIdentity`
- Senha (`-storepass`) para o keystore de identidade: `clientPwd`
- A chave de segurança (`-keypass`) para o keystore de identidade: `clientPwd`
- Certificado com base no keystore de identidade: `ClientCertificate.cer`
- Keystore confiável: `IBMUnicaTrust.jks`
- Senha (`-storepass`) para o keystore confiável: `trustPwd`

Os valores reais a serem inseridos devem ser específicos para sua instalação.

Para concluir etapas neste procedimento, execute o utilitário Java `keytool` a partir da linha de comandos.

Procedimento

1. Gere um keystore de identidade. Utilize o comando `genkey`, conforme mostrado no exemplo a seguir.

   O exemplo cria um keystore de identidade denominado `IBMUnicaClientIdentity.jks`. É possível utilizar um nome diferente para o keystore de identidade que você criar.

   ```
   keytool -genkey -alias IBMUnicaClientIdentity -keyalg RSA -keystore
   <IBMUnicaClientIdentity.jks> -keypass <clientPwd> -validity 1000 -dname
   "CN=hostName, O=myCompany" -storepass <clientPwd>
   ```

   Note o seguinte.

   - Utilize os valores para `alias`, `keystore`, `keypass` e `storepass` posteriormente neste procedimento e quando configurar o SSL no servidor de aplicativos da web.
   - Para o WebSphere 6.0, a senha do keystore (`-storepass`) e a senha da chave (`-keypass`) devem ser as mesmas.
   - No nome distinto (`-dname`), o nome comum (`CN`) é o mesmo nome do host utilizado para acessar o IBM EMM. Por exemplo, se o URL para IBM EMM for `https://hostName.example.com:7002/unica/jsp`, o CN será `hostName.example.com`. A parte de CN do nome distinto é a única parte necessária; Organização (`O`) e Unidade Organizacional (`UO`) não são necessários.

2. Gere um certificado com base no keystore de identidade. Utilize o comando `export`, conforme mostrado no exemplo a seguir.

   O exemplo gera um certificado denominado `ClientCertificate.cer`. É possível utilizar um nome diferente para o certificado que você criar.

   Os valores para `keystores`, `storepass` e `alias` devem corresponder aos valores especificados no keystore de identidade.

   ```
   keytool -export -keystore <IBMUnicaClientIdentity.jks> -storepass
   <clientPwd> -alias IBMUnicaClientIdentity -file <ClientCertificate.cer>
   ```

3. Gere o keystore confiável. Utilize o comando `import`, conforme mostrado no exemplo a seguir.

   O exemplo gera um keystore confiável denominado `IBMUnicaTrust.jks`. É possível utilizar um nome diferente para o keystore confiável que você criar.

   ```
   keytool –import -alias IBMUnicaClientIdentity -file
   <ClientCertificate.cer> -keystore <IBMUnicaTrust.jks> -storepass
   <trustPwd>
   ```

   Digite **Y** quando solicitado para confiar no certificado.

O que Fazer Depois

Observe os valores que foram definidos para as seguintes variáveis. Os valores podem ser diferentes dos valores fornecidos no exemplo.

- `alias` (no exemplo: `IBMUnicaClientIdentity`)
- `identity keystore` (no exemplo: `IBMUnicaClientIdentity.jks`)
- `storepass` (no exemplo: `trustPwd`) O valor de `storepass` para o keystore confiável pode ser diferente do valor de `storepass` para o keystore de identidade e certificado.

- `keystore` (no exemplo: `IBMUnicaTrust.jks`) Dependendo do servidor de aplicativos da web, você também especifica o keystore de identidade.

Defina esses valores específicos da instalação quando configurar o SSL no servidor de aplicativos da web para sua instalação do IBM EMM.

Configurando SSL ao utilizar o WebLogic

Esta seção descreve as etapas necessárias para configurar o SSL se implementar os componentes do IBM EMM no Oracle WebLogic. Esta mudança é necessária para permitir que componentes do eMessage que operam dentro do Campaign se comuniquem com o IBM EMM Hosted Services sobre SSL.

Sobre Esta Tarefa

Para obter orientação específica sobre como navegar e trabalhar com a interface com o usuário do Oracle WebLogic, consulte a documentação para a versão específica do Oracle WebLogic que estiver utilizando.

Procedimento

Conclua as tarefas a seguir.
- Modificar o script de inicialização do WebLogic
- Modificar a configuração do WebLogic
- Obter um certificado digital a partir do IBM EMM Hosted Services
- Criar um keystore confiável e importar o certificado digital do IBM

Modificando o script de inicialização do WebLogic

Se você implementou o Campaign no WebLogic, deve-se modificar o script de inicialização do WebLogic e a configuração do WebLogic para o SSL para que o WebLogic reconheça e aceite comunicação segura entre componentes do eMessage e do IBM EMM Hosted Services instalados localmente.

Procedimento

Inclua os seguintes argumentos em JAVA_OPTIONS no script de inicialização do WebLogic.
- `-Dweblogic.security.SSL.allowSmallRSAExponent=true`
- WebLogic versão 12c ou superior: `-Dweblogic.security.SSL.protocolVersion=TLS1`

  Todas as versões anteriores: `-Dweblogic.security.SSL.nojce=true`

Modificar a configuração do WebLogic

Você deve alterar a configuração SSL no WebLogic.

Procedimento

Utilize o console do WebLogic para fazer a seguinte mudança na configuração de SSL do WebLogic para seu domínio.
Altere a configuração para **Verificação de Nome do Host** para `Nenhuma`.

Obtendo um certificado a partir do IBM EMM Hosted Services

Para configurar a comunicação SSL, deve-se fazer download de um certificado digital a partir do IBM EMM Hosted Services. Os detalhes do certificado são salvos em um arquivo com a extensão `.cer` que pode ser importado no keystore do servidor de aplicativos da web.

Sobre Esta Tarefa

O acesso ao IBM EMM Hosted Services poderá ser perdido quando o certificado SSL existente expirar. Use este procedimento para fazer download de um novo certificado.

Procedimento

1. No Internet Explorer, efetue login no endereço para o IBM EMM Hosted Services que foi configurado para sua conta de email hospedada.
   - Para o datacenter dos EUA, acesse `https://em.unicaondemand.com`
   - Para o datacenter do Reino Unido, acesse `https://em-eu.unicaondemand.com`

   A tentativa de login resulta em um login com falha, mas permite utilizar o navegador para enviar a solicitação de certificado.
2. Clique no ícone de bloqueio e selecione **Visualizar Certificado**.
3. Selecione a guia Detalhes e selecione **Copiar para Arquivo**.

   Salve o arquivo com uma extensão `.cer` em um local que seja acessível para o servidor de aplicativos da web. O arquivo criado é o certificado digital que você insere no keystore no servidor de aplicativos da web.

   Por exemplo, salve o certificado como `IBMHosted.cer`.

Crie um armazenamento de confiança para o WebLogic e importe o certificado do IBM

Para Weblogic, você deve criar um keystore confiável que aceita o certificado IBM.

Antes de Iniciar

Antes de iniciar, utilize um navegador da web para fazer download do certificado digital do IBM EMM Hosted Services e salve-o como um arquivo `.cer`. Por exemplo, o certificado pode ser nomeado `IBMHosted.cer` (o nome do arquivo pode ser diferente). Para obter detalhes adicionais, consulte "Obtendo um certificado a partir do IBM EMM Hosted Services".

Sobre Esta Tarefa

A IBM utiliza os valores de amostra a seguir nos procedimentos contidos nesta seção.

- Keystore de identidade: `IBMUnicaClientIdentity.jks`
- A senha para o keystore de identidade: `clientPwd`
- Keystore confiável: `IBMUnicaTrust.jks`
- Alias para o keystore confiável: `IBMUnicaHostedIdentity`
- Senha (`-storepass`) para o keystore confiável: `trustPwd`
- Certificado digital (`-file`) de IBM: `IBMHosted.cer`

Os valores reais a serem inseridos devem ser específicos para sua instalação.

Para concluir etapas neste procedimento, execute o utilitário Java `keytool` a partir da linha de comandos.

Procedimento

1. Gere um keystore confiável para o WebLogic. Para obter detalhes, consulte "Gerando um keystore confiável" na página 26.

   Especifique o *identity keystore* e o *trusted keystore* na configuração do WebLogic.
2. Utilize o comando `import` no utilitário `keytool` para incluir o certificado IBM EMM Hosted Services no keystore confiável criado na Etapa 1, conforme mostrado no exemplo a seguir. Utilize o certificado digital que você transferiu por download a partir do IBM.

   Neste procedimento, você também define um alias para o keystore confiável.
   ```
   keytool -import -alias IBMUnicaHostedIdentity -file <IBMHosted.cer>
   -keystore <IBMUnicaTrust.jks> -storepass <trustPwd>
   ```
   Digite **Y** quando solicitado para confiar no certificado.
3. No console de administração do WebLogic, configure os keystores para o servidor.

   Para especificar as regras de configuração, selecione a opção para os keystores Identidade Customizada e Confiança Customizada a partir das opções disponíveis. Para a Identidade Customizada, especifique o keystore de identidade. Para a Confiança Customizada, especifique o keystore confiável.

   Por exemplo, no console de administração, especifique o seguinte (utilizando os valores de exemplo do keystore confiável criado na Etapa 1).
   - Para **Identidade**: especifique o keystore de identidade e a senha associada.

     Por exemplo, `IBMUnicaClientIdentity.jks` e `clientPwd`.
   - Para **Confiança**: especifique o keystore confiável e a senha associada.

     Por exemplo, `IBMUnicaTrust.jks` e `trustPwd`.

   Especifique o caminho completo para ambos os keystores.
4. Reinicie o WebLogic. O WebLogic não implementa as mudanças na configuração até reiniciar o servidor de aplicativos da web.
5. Para testar a conexão SSL, efetue login no IBM Campaign e acessar vários menus de recursos do sistema de mensagem. Confirme se é possível criar email, páginas de entrada e envios.

Configurando o SSL quando usar o IBM WebSphere

Esta seção descreve as etapas gerais necessárias para configurar o SSL se tiver implementado os componentes do IBM EMM no IBM WebSphere. Esta mudança é necessária para permitir que componentes do eMessage que operam dentro do Campaign se comuniquem com o IBM EMM Hosted Services sobre SSL.

Antes de Iniciar

Antes de iniciar, é necessário saber o valor para a propriedade de configuração do `uiHostName`. O valor para `uiHostName` é a URL para o IBM EMM Hosted Services. Para obter detalhes, consulte "Configurando os endereços utilizados para se conectar ao IBM EMM Hosted Services" na página 25.

Sobre Esta Tarefa

Deve-se acessar o console de segurança do WebSphere para modificar as configurações do gerenciamento de certificado SSL e de chaves. Esta tarefa requer um reinício do servidor de aplicativos da web do Campaign para implementar as mudanças.

Se tiver implementado o Campaign no WebSphere versão 6.1 ou superior, deve-se modificar a configuração de segurança do WebSphere para recuperar o certificado de assinante do IBM EMM Hosted Services e incluí-lo no armazenamento de confiança do WebSphere. Se receber uma mensagem de erro indicando que o certificado de assinante atual expirou, exclua o certificado atual e inclua um novo.

Para obter orientação específica sobre a navegação e trabalhar com a interface com o usuário do WebSphere, consulte a documentação da versão específica do IBM WebSphere que você está utilizando.

Nota: Antes de iniciar, confirme se o fix pack 7.0.0.17 foi instalado no servidor do WebSphere. Para obter informações adicionais, consulte o “O IBM WebSphere Application Server V7.0 requer o fixpack 7.0.0.17 ou superior” na página 32.

Procedimento

1. Gerar um keystore confiável.

   Para obter detalhes adicionais, consulte “Gerando um keystore confiável” na página 26.

   Para configurar o SSL, é necessário especificar os valores que são definidos para as seguintes variáveis. Os valores mostrados são apenas como exemplo. Os valores podem ser diferentes.

   - `alias`: *`UnicaClientIdentity`* (exemplo)
   - `keystore`: *`IBMUnicaTrust.jks`* (examplo)
   - `storepass`: *`trustPwd`* (exemplo)
2. Selecione o novo keystore no console de segurança do WebSphere.

   Por exemplo, se seguiu o exemplo na Etapa 1, selecione `IBMUnicaTrust.jks`.
3. Obtenha um certificado de segurança do IBM EMM Hosted Services e importe-o no WebSphere, conforme descrito nas etapas a seguir.
   a. No console de segurança do WebSphere, navegue até **Certificado SSL e gerenciamento de chave** > **Armazenamentos de chave e certificados** > **NodeDefaultTrustStore** > **Certificados de assinante**. Selecione a opção para **Recuperar da porta**.
   b. Configure WebSphere para estabelecer uma conexão de teste para recuperar o certificado de assinante do IBM EMM Hosted Services. Insira os seguintes valores para o certificado do assinante IBM EMM Hosted Services.
      - **Host** O valor que é definido para `eMessage >serverComponentsAndLocations > hostedServices >uiHostName`
      - **Porta** 443
      - **Configuração SSL para conexão de saída** `NodeDefaultSSLSettings`
      - **Alias** O valor inserido para **Host**

      Quando tiver concluído, WebSphere se comunica com o IBM EMM Hosted Services para recuperar as informações necessárias para criar um certificado de assinante para o IBM EMM Hosted Services.
4. Depois que o WebSphere concluir a criação do certificado de assinante, selecione o novo certificado no console de segurança.

O servidor de aplicativos da web utiliza o novo certificado ao estabelecer conexões com o IBM EMM Hosted Services.

5. Reinicie o WebSphere

   O WebSphere não implementa as mudanças na configuração até que você reinicie o servidor de aplicativos da web.

O IBM WebSphere Application Server V7.0 requer o fixpack 7.0.0.17 ou superior

Caso você planeje usar o IBM WebSphere Application Server V7.0 para implementar qualquer produto IBM EMM, aplique o Fix Pack 17 (também chamado de Versão 7.0.0.17) ou superior, para tratar de um problema de segurança. Isso se aplica a todos os pacotes do WebSphere Application Server 7.0, incluindo a versão que é compactada com alguns produtos do IBM EMM.

É possível obter o Fix Pack 17 ou posterior aqui:

http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg27013594.

Observe que, nessa página, deve-se selecionar o Fix Pack correto antes de fazer o download.

Para obter informações adicionais sobre versões suportadas do WebSphere para implementação de produtos IBM EMM, consulte o documento *Ambientes de Software Recomendados e Requisitos Mínimos do Sistema* para cada produto.

Capítulo 4. Operação Response and Contact Tracker

O Response and Contact Tracker (RCT) é instalado em seu ambiente local e se comunica com o IBM EMM Hosted Services para recuperar e processar dados para contatos de email, distribuição de emails e respostas de destinatários como cliques em links e aberturas. O RCT deve estar em execução para recuperar o rastreamento de link e dados de notificação de entrega de email do IBM EMM Hosted Services.

O Response and Contact Tracker (RCT) é instalado em seu ambiente local e se comunica com o IBM EMM Hosted Services para recuperar e processar dados para contatos de email, distribuição de emails e respostas de destinatários como cliques em links e aberturas. O RCT deve estar em execução para recuperar o rastreamento de link e dados de notificação de entrega de email do IBM EMM Hosted Services.

É possível iniciar o RCT de uma das seguintes maneiras.
- Iniciar o RCT manualmente.
- Iniciar o RCT como um serviço

Importante: Deve-se iniciar o RCT manualmente na primeira vez que utilizar o eMessage, mesmo se registrou o RCT como um serviço.

Deve-se reiniciar o RCT quando fizer mudanças nas propriedades de configuração para o eMessage. É possível reiniciar o RCT a qualquer momento, mesmo se tiver configurado-o para executar como um serviço. O IBM EMM Hosted Services continuará armazenando dados de rastreamento se o RCT for encerrado ou reiniciado. Quando ele continuar a operação, o RCT faz download das informações da fila.

Conceitos relacionados:

"Frequência de download de dados e configuração de porta" na página 23
"Início manual do RCT"
"Sobre como iniciar o RCT automaticamente como um serviço" na página 34

Início manual do RCT

Execute o script `rct` para iniciar e parar o Response and Contact Tracker (RCT). Para iniciar o RCT manualmente, execute o script `rct` no diretório `bin` em sua instalação do eMessage.

Para obter mais informações sobre esse script, consulte "O script RCT" na página 58.

Conceitos relacionados:

Capítulo 4, "Operação Response and Contact Tracker"

Operação manual do Response and Contact Tracker

Para operar o Response and Contact Tracker (RCT) manualmente, execute o script `rct` no diretório `bin` em sua instalação do eMessage.

Procedimento

- Para iniciar o RTC, execute o script `rct` no diretório `bin` em sua instalação do eMessage, da seguinte maneira.

  `rct start`
- Para parar o RCT, execute o script `rct` da seguinte maneira.

  `rct stop`

O que Fazer Depois

Para obter mais informações sobre esse script, consulte "O script RCT" na página 58.

Parando o Response and Contact Tracker

Pare o Response and Contact Tracker (RCT) executando o script `rct`.

Procedimento

No diretório `bin` de sua instalação do eMessage, execute o script `rct` da seguinte forma:
`rct stop`

O que Fazer Depois

O IBM EMM Hosted Services continua a armazenar dados de rastreamento e resposta que ele recebe até reiniciar o RCT.

Para obter mais informações sobre esse script, consulte "O script RCT" na página 58

Sobre como iniciar o RCT automaticamente como um serviço

É possível configurar o Response and Contact Tracker (RCT) para iniciar automaticamente incluindo-o como um serviço.

Registre o serviço do RCT executando o script `MKService_rct` que é fornecido com o software eMessage.

Quando executar o script `MKService_rct` para registrar o serviço, deve-se utilizar o script `rct` para iniciar manualmente o RCT pela primeira vez. Depois isso, o RCT será reiniciado automaticamente toda vez que reinicializar o sistema operacional da máquina em que instalou o RCT.

Após configurar o serviço RCT, é possível impedir que o RCT seja iniciado automaticamente executando o script `MKService_rct` com a opção `-remove`.

Conceitos relacionados:

Capítulo 4, "Operação Response and Contact Tracker", na página 33

Tarefas relacionadas:

"Incluindo o Response and Contact Tracker como um serviço" na página 35

"Removendo o serviço Response and Contact Tracker" na página 35

Referências relacionadas:

"O script MKService_rct" na página 59

Incluindo o Response and Contact Tracker como um serviço

É possível configurar o Response and Contact Tracker (RCT) para iniciar automaticamente incluindo-o como um serviço.

Sobre Esta Tarefa

Registre o serviço do RCT executando o script `MKService_rct` que é fornecido com o software eMessage.

Para incluir o Response and Contact Tracker (RCT) como um serviço, execute o script `MKService_rct -install` a partir do diretório `bin` em sua instalação do eMessage.

O diretório `bin` é criado como um subdiretório no diretório de instalação do Campaign quando você instala ou faz upgrade para a versão mais recente de IBM Campaign.

Procedimento

Para incluir o Response and Contact Tracker (RCT) como um serviço, execute o script `MKService_rct -install` a partir do diretório `bin` em sua instalação do eMessage.
No UNIX ou Linux, execute este script com um usuário que possua permissões de raiz ou permissões para criar processos daemon.
No Windows, o nome do serviço é **Response & Contact Tracker**.

O que Fazer Depois

Após executar o script `MKService_rct`, inicie o RCT manualmente com o script `rct`. Reinicie manualmente o RCT apenas uma vez. Após iniciar o RCT manualmente na primeira vez, o RCT será reiniciado automaticamente toda vez que reiniciar o sistema operacional do computador no qual instalou o RCT.

Após configurar o serviço RCT, é possível impedir que o RCT seja iniciado automaticamente executando o script `MKService_rct` com a opção `-remove`.

Conceitos relacionados:

"Sobre como iniciar o RCT automaticamente como um serviço" na página 34

Referências relacionadas:

"O script MKService_rct" na página 59

"O script RCT" na página 58

Removendo o serviço Response and Contact Tracker

Se instalou o Response and Contact Tracker (RCT) como um serviço, o RCT será reiniciado sempre que reiniciar o sistema no qual instalou o RCT. Para evitar que o RCT reinicie automaticamente, você deve remover o serviço Response and Contact Tracker (RCT).

Procedimento

Para remover o RCT como um serviço, execute o script `MKService_rct` com a opção `-remove`.
A partir de uma linha de comandos Windows, em seu diretório inicial do IBM

EMM, execute `eMessage\bin\MKService_rct.bat -remove`.
No UNIX ou Linux, em seu diretório inicial do IBM EMM, execute `eMessage/bin/MKService_rct.sh -remove`.

O que Fazer Depois

Para obter mais informações sobre esse script, consulte "O script MKService_rct" na página 59

Conceitos relacionados:

"Sobre como iniciar o RCT automaticamente como um serviço" na página 34

Capítulo 5. Verificação de inicialização

Para assegurar o acesso a todos os recursos de email hospedado, teste as configurações e conexões para suas instalações do Campaign e eMessage após ativar o eMessage, expanda sua instalação do eMessage ou faça upgrade da instalação do Campaign.

Verifique as configurações e conexões após executar um dos itens a seguir.

- Ativar o eMessage pela primeira vez
- Fazer upgrade de sua instalação atual do IBM Campaign
- Incluir uma nova partição na configuração do eMessage mantida no IBM Marketing Platform

Confirmação para configurações do sistema

Para assegurar que as preparações de inicialização estejam concluídas, confirme se as propriedades de configuração a seguir estão configuradas e se atendem aos requisitos para suas instalações do eMessage e Campaign.

Propriedade de Configuração	**Configuração**
`Campaign | partitions | partition[n] | eMessage | eMessagePluginJarFile`	Caminho completo para o local do arquivo de plug-in que opera como o Recipient List Uploader (RLU). Insira o caminho do diretório local completo no sistema de arquivos para o computador que hospeda o servidor de aplicativos da web do Campaign. O instalador do IBM preenche esta configuração automaticamente para a partição padrão quando executar o instalador. Para outras partições, configure esta propriedade manualmente.
`Campaign | partitions | partition[n] | server | internal | eMessageInstalled`	Indica que o eMessage está instalado. Configure esta propriedade como **Sim** em cada partição na qual desejar ativar o eMessage, incluindo a partição padrão. Quando configurar esta propriedade como **Sim**, os recursos do eMessage ficarão disponíveis na interface do Campaign.
`eMessage | serverComponentsAndLocations | hostedServices | uiHostName`	Endereço para o IBM EMM Hosted Services para todas as comunicações, exceto listas de upload. A configuração padrão é `em.unicaondemand.com` para o datacenter dos EUA. Se você estiver conectando ao datacenter no Reino Unido, altere este valor para `em-eu.unicaondemand.com`.
`eMessage | serverComponentsAndLocations | hostedServices | dataHostName`	O endereço para a conexão que o eMessage usa para fazer upload dos metadados que estão relacionados a listas de destinatários para o IBM EMM Hosted Services. A configuração padrão é `em.unicaondemand.com` para o datacenter dos EUA. Se você estiver conectando ao datacenter no Reino Unido, altere este valor para `em-eu.unicaondemand.com`.

<table>
<tr><th>Propriedade de Configuração</th><th>Configuração</th></tr>
<tr><td>eMessage | serverComponentsAndLocations | hostedServices | ftpHostName</td><td>O endereço para a conexão que o eMessage usa para upload de dados da lista de destinatários (exceto metadados de lista) para o IBM EMM Hosted Services.

A configuração padrão é ftp-em.unicaondemand.com para o datacenter dos EUA.

Se estiver conectando ao datacenter no Reino Unido, altere este valor para ftp-em-eu.unicaondemand.com.</td></tr>
<tr><td>eMessage | partitions | partition[n] | hostedAccountInfo | amUserForAcctCredentials</td><td>O usuário do IBM EMM que faz referência à origem de dados que contém as credenciais de acesso do IBM EMM Hosted Services.

Configure esse valor quando criar um usuário do sistema para acessar os recursos de email hospedados pelo IBM.</td></tr>
<tr><td>eMessage | partitions | partition[n] | hostedAccountInfo | amDataSourceForAcctCredentials</td><td>A origem de dados do Marketing Platformque contém as credenciais de login do IBM EMM Hosted Services.

Configure esse valor quando criar um usuário do sistema para acessar os recursos de email hospedados pelo IBM.</td></tr>
<tr><td>eMessage | partitions | partition [n] < dataSources | systemTables | type</td><td>Tipo de banco de dados que hospeda as tabelas do sistema.

Forneça o valor correto para seu banco de dados.</td></tr>
<tr><td>eMessage | partitions | partition [n] < dataSources | systemTables | schemaName</td><td>Nome do esquema do banco de dados para as tabelas de sistema.

Configure para o nome do esquema apropriado para seu banco de dados.</td></tr>
<tr><td>eMessage | partitions | partition [n] < dataSources | systemTables | jdbcClassName</td><td>Driver JDBC para tabelas de sistema.

Forneça o valor correto para seu ambiente.</td></tr>
<tr><td>eMessage | partitions | partition [n] < dataSources | systemTables | jdbcURI</td><td>URI de conexão JDBC para tabelas de sistema.

Forneça o valor correto para seu ambiente.

Especifique o tipo de banco de dados, driver de banco de dados, host, porta e o nome do banco de dados. Por exemplo: jdbc:oracle:thin:@yourdb.example.com:1234:DBname

Consulte sua documentação do banco de dados para obter instruções específicas sobre como construir a URL do JDBC.

O valor que inserir deve corresponder exatamente ao valor definido em seu servidor da web do Campaign.</td></tr>
<tr><td>eMessage | partitions | partition [n] < dataSources | systemTables | asmUserForDBCredentials</td><td>O usuário do IBM EMM que faz referência à origem de dados que contém as credenciais de login da tabela de sistema.

É possível criar esse usuário quando configurar o acesso às tabelas de sistema do eMessage locais.</td></tr>
<tr><td>eMessage | partitions | partition [n] < dataSources | systemTables | asmDataSourceForDBCredentials</td><td>A origem de dados do Marketing Platform que contém as credenciais de login para o banco de dados que contém as tabelas do sistema.

É possível criar esta origem de dados quando criar um usuário para acessar as tabelas de sistema do eMessage.</td></tr>
</table>

Conceitos relacionados:

Capítulo 6, “Configurações para o IBM eMessage”, na página 41

Tarefas relacionadas:

“Configurando o usuário do sistema que acessa o IBM EMM Hosted Services” na página 23

"Configurando o acesso às tabelas do sistema local do eMessage" na página 45

Testando upload para o IBM EMM Hosted Services

Para testar a capacidade de fazer upload para o IBM EMM Hosted Services a partir de seu ambiente local, o script `rlu` no modo de verificação.

Procedimento

No diretório `bin` em sua instalação do eMessage, execute o script `rlu` em uma das formas a seguir.

- `rlu -c`
- `rlu --check`

Referências relacionadas:

"O script do RLU" na página 57

Testando download a partir do IBM EMM Hosted Services

Para testar a capacidade de fazer o download das informações a partir do IBM EMM Hosted Services, execute o script `rct` em modo de verificação.

Procedimento

No diretório `bin` de sua instalação do eMessage, execute o script `rct` da seguinte forma:
`rct check`

Referências relacionadas:

"O script RCT" na página 58

Testando a conexão com a interface do sistema de mensagens hospedado

O IBM hospeda a interface do sistema de mensagens a partir de seus datacenters nos Estados Unidos e no Reino Unido. Teste a conexão com a interface de correspondência hospedada tentando acessar um recurso do eMessage.

Procedimento

Efetue login no IBM EMM e selecione **Correspondências do eMessage** no menu **Campaign**.
Se a conexão com a interface com o usuário do eMessage for estabelecida corretamente, a página de correspondências do eMessage é aberta exibindo uma lista de correspondências e características de correspondências relacionadas.
Se a conexão com a interface com o usuário não for estabelecida adequadamente, um erro será exibido.

Capítulo 6. Configurações para o IBM eMessage

O IBMMarketing Platform fornece várias propriedades de configuração para modificar o comportamento e a aparência do IBMeMessage. Algumas propriedades de configuração são definidas durante a instalação. É possível alterar as propriedades de configuração a qualquer momento.

Após atualizar as configurações do Campaign ou eMessage, você deve reiniciar o Response and Contact Tracker (RCT) e o servidor de aplicativos da web que hospeda o Campaign.

Característica ou Recurso	Propriedade de configuração (incluindo caminho)
Ativar ou desativar o eMessage na partição do Campaign. Consulte o "Campanha	Partições	Partição[n]	Servidor	Interno" na página 47.	`Campaign | Partições | Partição[n] | Servidor | Interno`
Características de listas de destinatários de email. Consulte o "Campanha	Partições	Partição[n]	eMessage" na página 46.	`Campanha | Partições | Partição[n] | eMessage`
URLs necessárias para se conectar ao IBM EMM Hosted Services. Consulte o "eMessage	serverComponentsAndLocations	hostedServices" na página 50.	`eMessage | serverComponentsAndLocations | hostedServices`
Credenciais de acesso ao banco de dados e de conta para se conectar ao IBM EMM Hosted Services. Consulte "eMessage	partitions	partition[n]	hostedAccountInfo" na página 51	`eMessage | partitions | partition[n] | hostedAccountInfo`
Configurações de acesso e de esquema do banco de dados para as tabelas de sistema do eMessage. Consulte "eMessage	Partições	Partição[n]	dataSources	systemTables" na página 52	`eMessage | partitions | partition[n] | dataSources | systemTables`
Local de um script que é executado em resposta às ações ou status do Recipient List Uploader. (opcional) Consulte "eMessage	partitions	partition[n]	recipientListUploader" na página 55	`eMessage | partitions | partition[n] | recipientListUploader`

Característica ou Recurso	Propriedade de configuração (incluindo caminho)
Configurações relacionadas ao download de dados, processadas pelo Response and Contact Tracker (RCT). Consulte "eMessage	Partições	Partição[n]	responseContactTracker" na página 55	`eMessage	partitions	partition[n]	responseContactTracker`
Suporte para apresentar listas de dados personalizados em eMessage com base nas tabelas de dimensões no Campaign. Consulte Configurando o suporte para tabelas de dimensões.	`Campaign	partitions	partition[n]	eMessage	oltDimTableSupport`
Suporte para rastreamento de histórico da execução da correspondência. Consulte "eMessage	Partições	Partição[n]	responseContactTracker" na página 55	`eMessage	partitions	partition[n]	responseContactTracker` Consulte o parâmetro **enableExecutionHistoryDataTracking**.

Para obter mais informações sobre trabalhar com propriedades de configuração, consulte o *IBM Marketing Platform Administrator's Guide*.

Conceitos relacionados:

"Confirmação para configurações do sistema" na página 37

o que é possível configurar para o eMessage

É possível configurar os seguintes aspectos do local do IBM eMessage.

Característica ou Recurso	Propriedade de configuração (incluindo caminho)
Ativar ou desativar o eMessage na partição do Campaign. Consulte o "Campanha	Partições	Partição[n]	Servidor	Interno" na página 47.	`Campaign	Partições	Partição[n]	Servidor	Interno`
Características de listas de destinatários de email. Consulte o "Campanha	Partições	Partição[n]	eMessage" na página 46.	`Campanha	Partições	Partição[n]	eMessage`
URLs necessárias para se conectar ao IBM EMM Hosted Services. Consulte o "eMessage	serverComponentsAndLocations	hostedServices" na página 50.	`eMessage	serverComponentsAndLocations	hostedServices`
Credenciais de acesso ao banco de dados e de conta para se conectar ao IBM EMM Hosted Services. Consulte "eMessage	partitions	partition[n]	hostedAccountInfo" na página 51	`eMessage	partitions	partition[n]	hostedAccountInfo`

Característica ou Recurso	Propriedade de configuração (incluindo caminho)
Configurações de acesso e de esquema do banco de dados para as tabelas de sistema do eMessage. Consulte "eMessage	Partições	Partição[n]	dataSources	systemTables" na página 52	`eMessage | partitions | partition[n] | dataSources | systemTables`
Local de um script que é executado em resposta às ações ou status do Recipient List Uploader. (opcional) Consulte "eMessage	partitions	partition[n]	recipientListUploader" na página 55	`eMessage | partitions | partition[n] | recipientListUploader`
Configurações que são relacionadas ao download de dados, processado pelo Response and Contact Tracker (RCT). Consulte "eMessage	Partições	Partição[n]	responseContactTracker" na página 55	`eMessage | partitions | partition[n] | responseContactTracker`
Suporte para apresentar listas de dados personalizados em eMessage com base nas tabelas de dimensões no Campaign. Consulte o "Configurando suporte para tabelas de dimensão" na página 44.	`Campaign | partitions | partition[n] | eMessage | oltDimTableSupport`

O que reiniciar após as mudanças na configuração

Após fazer mudanças nas configurações do Campaign ou do eMessage, deve-se reiniciar o Response and Contact Tracker (RCT) e o servidor de aplicativos da web que hospeda o Campaign.

Para obter informações sobre como reiniciar o RCT, consulte "O script RCT" na página 58.

Para obter informações sobre como reiniciar o servidor de aplicativos da web, consulte a documentação para seu servidor de aplicativos da web.

Configurando o acesso ao histórico de execução da correspondência adicional

É possível solicitar que o IBM forneça dados adicionais para o histórico de execução da correspondência. O acesso aos dados adicionais do histórico de execução da correspondência é disponibilizado pela solicitação do IBM e ao atualizar a configuração do eMessage. Os dados do histórico de execução da correspondência são registrados nas do sistema eMessage na tabela `UACE_ExecHistory` para descrever execuções da correspondência concluídas.

Antes de Iniciar

Para fazer download de dados de execução de distribuição adicionais, deve-se atualizar a propriedade de configuração `enableExecutionHistoryDataTracking`. Por padrão, o `enableExecutionHistoryDataTracking` não é exposto nas propriedades de configuração eMessage.

É possível exibir essa propriedade de configuração em sua instalação local do eMessage executando o script `switch_config_visibility.bat` que está no diretório `emessage\tools`.

Sobre Esta Tarefa

Os seguintes tipos de registros estão disponíveis se você instalar ou atualizar o Campaign versão 8.6.0.4.

- Linha de assunto da mensagem
- Endereço de origem
- O usuário que atualizou a correspondência
- Descrição do documento
- Data de salvamento da correspondência

Procedimento

1. Solicite acesso aos dados do histórico de execução da correspondência adicionais. Para solicitar o acesso, entre em contato com seu representante IBM pelo email `eacctsvc@us.ibm.com`.
2. Atualize a configuração do eMessage. Configure a propriedade de configuração a seguir.

`Affinium|eMessage|partitions|partition1|responseContactTracker|`
`enableExecutionHistoryDataTracking`

Configure **`enableExecutionHistoryDataTracking`** para **true**.

O que Fazer Depois

É possível consultar as tabelas de sistema do eMessage para recuperar as informações de execução da correspondência da tabela `UACE_ExecHistory`.

Para obter mais informações sobre as tabelas de sistema do eMessage, consulte o *Dicionário de Tabelas e Dados do Sistema IBM EMM*.

Tarefas relacionadas:

"Acessando os parâmetros de configuração para upload de FTP implícito" na página 16

Configurando suporte para tabelas de dimensão

Para suportar certos recursos que são fornecidos pelos scripts avançados para email, a propriedade de configuração `oltDimTableSupport` deve ser configurada como **True**. Ao atualizar para Campaign 8.5.0 ou mais recente, deve-se alterar o valor desta definição de configuração manualmente.

Sobre Esta Tarefa

O eMessage fornece scripts avançados para criar mensagens de email que exibem listas de informações personalizadas. Essas listas requerem associação de tabelas de dimensões criadas no Campaign com uma Tabela da Lista de Saída (OLT) que define a lista de destinatários de email. As Tabelas da Lista de Saída são criadas no esquema do eMessage.

A propriedade de configuração `oltDimTableSupport` controla o suporte para criação de tabelas de dimensões no esquema do eMessage . Quando o valor para esta propriedade é configurado como `True`, uma OLT pode utilizar as informações fornecidas em uma tabela de dimensões. Antes do Campaign 8.5.0, o valor padrão para `oltDimTableSupport` era `False` e não `True`.

Conclua as etapas a seguir para atualizar a propriedade `oltDimTableSupport`.

Para obter mais informações sobre como os comerciantes usam scripts avançados para criar tabelas de dados, consulte o *Guia do Usuário do IBM eMessage* .

Procedimento

1. Acesse **Configurações** > **Configuração** > **Campanha** > **Partições** > **partição [n]** > **eMessage**
2. Clique em **Editar configurações** e configure o valor da `propriedade oltDimTableSupport` para `True`.

Configurando o acesso às tabelas do sistema local do eMessage

Os componentes do eMessage devem ser capazes de acessar as tabelas de sistema eMessage no esquema do Campaign. Deve-se criar e configurar um usuário do sistema que possa acessar as tabelas do sistema automaticamente. O usuário do sistema que foi configurado durante a instalação do Campaign já possui o acesso necessário ao esquema do Campaign.

Sobre Esta Tarefa

Nota: Se a sua instalação contiver várias partições, deve-se concluir esta tarefa para cada partição. Não é possível compartilhar usuários do sistema nas partições.

Se desejar utilizar um usuário do sistema diferente para acessar as tabelas de sistema do eMessage, deve-se criar um novo usuário do sistema no Marketing Platform e criar uma nova origem de dados de plataforma com acesso ao esquema do Campaign.

Procedimento

1. Na configuração do eMessage, especifique um usuário do sistema que acesse o banco de dados que hospeda o esquema do Campaign.

   É possível criar um novo usuário ou especificar um usuário existente. O usuário do sistema que você configurou para o Campaign já possui acesso ao esquema do Campaign.

   Utilize a propriedade de configuração `eMessage > partitions > partition [n] < dataSources > systemTables > asmUserForDBCredentials.`.

   Por padrão, o usuário especificado é `asm_admin`.
2. Na configuração do eMessage, especifique a origem de dados que é configurada para conter o nome do usuário e senha necessários para acessar o banco de dados que hospeda o esquema do Campaign.

   É possível utilizar a origem de dados que foi criada para acessar o esquema do Campaign quando instalou o Campaign.

   Utilize a propriedade de configuração `eMessage > partitions > partition [n] < dataSources > systemTables > amDataSourceForDBCredentials`.

Conceitos relacionados:

"Confirmação para configurações do sistema" na página 37

Propriedades de configuração do eMessage

Acesse as propriedades de configuração do eMessage no menu Configurações no Marketing Platform. As propriedades para configurar o eMessage estão contidas nas categorias de configuração do Campaign e eMessage.

Para acessar as propriedades de configuração, navegue para **Configurações > Configurações**. A página Configurações lista todas as propriedades de configuração disponíveis para sua instalação do IBM EMM.

Campanha | Partições | Partição[n] | eMessage

Defina propriedades nesta categoria para definir características de listas de destinatários e especifique o local de recursos que fazem upload das listas para o IBM EMM Hosted Services.

eMessagePluginJarFile

Descrição

Caminho completo para o local do arquivo que opera como RLU (Recipient List Uploader). Este plug-in para o Campaign faz upload dos dados da OLT e os metadados associados aos serviços remotos hospedados pelo IBM. O local que especificar deve ser o caminho de diretório local integral no sistema de arquivos para o computador que hospeda o servidor de aplicativos da web do Campaign.

O instalador do IBM preenche esta configuração automaticamente para a partição padrão quando executar o instalador. Para outras partições, deve-se configurar esta propriedade manualmente. Como há apenas um RLU para cada instalação do eMessage, todas as partições devem especificar o mesmo local para o RLU.

Não altere essa configuração a menos que o IBM o instrua a fazer isso.

Valor Padrão

Nenhum valor padrão definido.

Valores válidos

Caminho do diretório local integral onde instalou o servidor da web do Campaign.

defaultSeedInterval

Descrição

O número de mensagens entre mensagens iniciais se `defaultSeedType` for `Distribuir lista`.

Valor Padrão

`1000`

defaultSeedType

Descrição

O método padrão que o eMessage usa para inserir endereços iniciais em uma lista de destinatários.

Valor Padrão

`Distribuir IDs`

Valores válidos

- `Distribuir IDS` - Distribui IDs igualmente, com base no tamanho da lista de destinatários e no número de endereços de valor inicial disponíveis, e insere endereços de valor inicial em intervalos iguais em toda a lista de destinatários.
- `Distribuir lista` - Insere o endereço do valor inicial para cada ID `defaultSeedInterval` na lista principal. Insere a lista inteira de endereços iniciais disponíveis em intervalos especificados por toda a lista de destinatários. Você deve especificar o intervalo entre pontos de inserção.

oltTableNamePrefix

Descrição

Usado no esquema gerado para a tabela da lista de saída. Você deve definir esse parâmetro.

Valor Padrão

OLT

Valores válidos

O prefixo não pode conter mais de 8 caracteres alfanuméricos ou de sublinhado, e deve iniciar com uma letra.

oltDimTableSupport

Descrição

Este parâmetro de configuração controla a capacidade de incluir tabelas de dimensões para Tabelas de Lista de Saída (OLT) criadas no esquema do eMessage. As tabelas de dimensões precisam usar script avançado para email para criar tabelas de dados em mensagens de email.

A configuração padrão é `False`. Você deve configurar esta propriedade como `True` para que os comerciantes possam criar tabelas de dimensões quando usam o processo do eMessage para definir uma lista de destinatários. Para obter mais informações sobre criar tabelas de dados e trabalhar com scripts avançados para email, consulte o *IBM eMessage User's Guide.*

Valor Padrão

False

Valores válidos

True | False

Campanha | Partições | Partição[n] | Servidor | Interno

As propriedades nessa categoria especificam as configurações de integração e os limites de internalID para a partição do Campaign selecionada. Se a sua instalação do Campaign tiver diversas partições, configure essas propriedades para cada partição que desejar afetar.

internalIdLowerLimit

Descrição

As propriedades `internalIdUpperLimit` e `internalIdLowerLimit` restringem os IDs internos do Campaign para estarem dentro do intervalo especificado. Observe que os valores são inclusivos: ou seja, o Campaign pode usar tanto o limite inferior quanto superior.

Valor Padrão

`0` (zero)

internalIdUpperLimit

Descrição

As propriedades `internalIdUpperLimit` e `internalIdLowerLimit` restringem os IDs internos do Campaign para estarem dentro do intervalo especificado. Os valores são inclusivos, isto é, o Campaign pode usar o limite inferior e superior. Se o Distributed Marketing estiver instalado, configure o valor como `2147483647`.

Valor Padrão

`4294967295`

eMessageInstalled

Descrição

Indica que o eMessage está instalado. Ao selecionar `yes`, os recursos do eMessage ficam disponíveis na interface do Campaign.

O instalador do IBM configura essa propriedade como `yes` para a partição padrão em sua instalação do eMessage. Para partições adicionais em que o eMessage tenha sido instalado, deve-se configurar essa propriedade manualmente.

Valor Padrão

`no`

Valores válidos

`yes | no`

interactInstalled

Descrição

Após a instalação do ambiente de design do Interact, essa propriedade de configuração deve ser configurada como `yes` para ativar o ambiente de design do Interact no Campaign.

Se não tiver o Interact instalado, configure como `no`. A configuração dessa propriedade como `no` não remove os menus e as opções do Interact da interface com o usuário. Para remover menus e opções, deve-se cancelar manualmente o registro do Interact usando o utilitário `configTool`.

Valor Padrão

no

Valores válidos

yes | no

Disponibilidade

Esta propriedade é aplicável apenas se o Interact tiver sido instalado.

MO_UC_integration

Descrição

Ativa a integração com o Marketing Operations para esta partição. Se você planeja configurar qualquer uma das três seguintes opções para Yes, deve configurar **MO_UC_integration** para Yes. Para obter mais informações sobre a configuração dessa integração, consulte o Guia de Integração do *IBM Marketing Operations e do Campaign*.

Valor Padrão

no

Valores válidos

yes | no

MO_UC_BottomUpTargetCells

Descrição

Permite células ascendentes para Planilhas de Célula de Destino nessa partição. Quando configurada como Yes, tanto células de destino de cima para baixo quanto de baixo para cima são visíveis, mas as células de destino de baixo para cima são somente de leitura. Note que **MO_UC_integration** deve ser ativado. Para obter mais informações sobre como configurar essa integração, consulte o Guia de Integração do *IBM Marketing Operations e do Campaign*.

Valor Padrão

no

Valores válidos

yes | no

Legacy_campaigns

Descrição

Quando a propriedade**MO_UC_integration** está configurada para **Yes**, a propriedade **Legacy_campaigns** ativa o acesso às campanhas criadas antes da ativação da integração, incluindo campanhas criadas no Campaign 7.x e vinculadas a projetos do Plan 7.x. Para obter mais informações sobre como configurar essa integração, consulte o Guia de Integração do *IBM Marketing Operations e do Campaign*.

Valor Padrão

no

Valores válidos

yes | no

IBM Marketing Operations - Integração da oferta

Descrição

Ativa a capacidade de usar o Marketing Operations para executar tarefas de gerenciamento do ciclo de vida da oferta nesta partição. (**MO_UC_integration** deve ser ativado. Além disso, a **Integração de campanhas** deve ser ativada em **Definições > Configuração > Unica > Plataforma**.) Para obter mais informações sobre como configurar essa integração, consulte o Guia de Integração do *IBM Marketing Operations e do Campaign*.

Valor Padrão

no

Valores válidos

yes | no

UC_CM_integration

Descrição

Ativa a integração de segmento online do Digital Analytics para uma partição do Campaign. Se você configurar essa opção para yes, a caixa Selecionar processo em um fluxograma fornecerá a opção de selecionar os **Digital Analytics Segmentos** como entrada. Para configurar a integração para cada partição, escolha **Definições > Configuração > Campaign | partições | partição[n] | Coremetrics**.

Valor Padrão

no

Valores válidos

yes | no

eMessage | serverComponentsAndLocations | hostedServices

Defina propriedades para especificar as URLs para se conectar ao IBM EMM Hosted Services. O eMessage usa conexões separadas para fazer upload das listas de destinatários, metadados que descrevem listas de destinatários e para a comunicação em geral enviada ao ambiente hospedado.

Você deve alterar os valores padrão se estiver conectando-se ao IBM EMM Hosted Services por meio do datacenter que é estabelecido pelo IBM no Reino Unido. Consulte o IBM para determinar o datacenter ao qual você está conectado.

uiHostName

Descrição

O endereço que o eMessage usa para toda a comunicação com o IBM EMM Hosted Services, exceto o upload de listas de destinatários e metadados relacionados.

Valor Padrão

`em.unicaondemand.com`

Se você estiver se conectando ao datacenter do Reino Unido, altere este valor para `em-eu.unicaondemand.com`.

dataHostName

Descrição

O endereço que o eMessage usa para fazer upload dos metadados relacionados a listas de destinatários para o IBM EMM Hosted Services.

Valor Padrão

`em.unicaondemand.com`

Se você estiver se conectando ao datacenter do Reino Unido, altere este valor para `em-eu.unicaondemand.com`.

ftpHostName

Descrição

O endereço que o eMessage usa para fazer upload de dados relacionados às listas de destinatários (exceto metadados de lista) para o IBM EMM Hosted Services.

Valor Padrão

`ftp-em.unicaondemand.com`

Se você estiver se conectando ao datacenter do Reino Unido, altere este valor para `ftp-em-eu.unicaondemand.com`.

eMessage | partitions | partition[n] | hostedAccountInfo

Defina propriedades nesta categoria para definir credenciais de usuário para o banco de dados que contém informações da conta que são necessárias para acessar o IBM EMM Hosted Services. Os valores que você especifica aqui devem ser definidos como configurações do usuário no Marketing Platform.

amUserForAcctCredentials

Descrição

Use esta propriedade para especificar o usuário do Marketing Platform que contém uma origem de dados do Marketing Platform que especifica as credenciais de acesso da conta necessárias para acessar o IBM EMM Hosted Services.

Valor Padrão

asm_admin

Valores válidos

Qualquer usuário do Marketing Platform.

amDataSourceForAcctCredentials

Descrição

Use esta propriedade para especificar a origem de dados do Marketing Platform que define as credenciais de login para IBM EMM Hosted Services.

Valor Padrão

UNICA_HOSTED_SERVICES

Valores válidos

Uma origem de dados que é associada ao usuário que você especifica em `amUserForAcctCredentials`

eMessage | Partições | Partição[n] | dataSources | systemTables

Esta categoria contém propriedades de configuração que definem o esquema, as configurações de conexão e as credenciais de login para o banco de dados que contêm as tabelas de sistema do eMessage em seu ambiente de rede local.

type

Descrição

Tipo de banco de dados que hospeda as tabelas de sistema do eMessage.

Valor Padrão

Nenhum valor padrão definido. Você deve definir essa propriedade.

Valores válidos

- `SQLSERVER`
- `ORACLE9`
- `ORACLE10` (também usada para indicar bancos de dados Oracle 11)
- `DB2`

schemaName

Descrição

Nome o esquema do banco de dados para as tabelas de sistema do eMessage. Esse nome é igual ao nome do esquema para as tabelas de sistema do Campaign.

Deve-se incluir esse nome de esquema ao referenciar tabelas de sistema em scripts.

Valor Padrão

dbo

jdbcBatchSize

Descrição

O número de solicitações de execução JDBC executadas no banco de dados por vez.

Valor Padrão

10

Valores válidos

Um número inteiro maior que 0.

jdbcClassName

Descrição

O driver JDBC para tabelas de sistema como definido em seu servidor da web do Campaign.

Valor Padrão

Nenhum valor padrão definido. Você deve definir essa propriedade.

jdbcURI

Descrição

A URI de conexão JDBC para tabelas de sistema conforme definido em seu servidor da web do Campaign.

Valor Padrão

Nenhum valor padrão definido. Você deve definir essa propriedade.

asmUserForDBCredentials

Descrição

Use essa propriedade para especificar um usuário do sistema que tem permissão para acessar as tabelas de sistema do eMessage.

Valor Padrão

Nenhum valor padrão definido. Você deve definir essa propriedade.

Valores válidos

Qualquer usuário que está definido no Marketing Platform. Este usuário geralmente é o nome do usuário do sistema para o Campaign

amDataSourceForDBCredentials

Descrição

Use esta propriedade para especificar a origem de dados que define as credenciais de login para o banco de dados que contém as tabelas de sistema do eMessage. Essa origem de dados pode ser a mesma que a origem de dados para as tabelas de sistema do Campaign.

Valor Padrão

UA_SYSTEM_TABLES

Valores válidos

Uma origem de dados do Marketing Platform que está associada ao usuário que você especificar para o IBM EMM `asmUserForDBCredentials`.

A origem de dados especifica um usuário do banco de dados e as credenciais que são utilizadas para acessar as tabelas de sistema do eMessage. Se o esquema padrão para o usuário do banco de dados não contiver as tabelas de sistema, deve-se especificar o esquema da tabela de sistema na conexão JDBC que é utilizado para acessar as tabelas do sistema.

poolAcquireIncrement

Descrição

Quando o conjunto de conexões com o banco de dados esgotar as conexões, o número de novas conexões que eMessage cria para as tabelas de sistema. O eMessage cria novas conexões até o número especificado em `poolMaxSize`.

Valor Padrão

1

Valores válidos

Um número inteiro maior que 0.

poolIdleTestPeriod

Descrição

O número de segundos por que o eMessage aguarda entre conexões inativas de teste com as tabelas de sistema do eMessage para atividade.

Valor Padrão

100

Valores válidos

Um número inteiro maior que 0.

poolMaxSize

Descrição

O número máximo de conexões que o eMessage estabelece com as tabelas de sistema. Um valor de zero (0) indica que não há máximo.

Valor Padrão

100

Valores válidos

Um número inteiro maior que ou igual a 0.

poolMinSize

Descrição

O número mínimo de conexões que o eMessage estabele com as tabelas de sistema.

Valor Padrão

10

Valores válidos

Um número inteiro maior que ou igual a 0.

poolMaxStatements

Descrição

O número máximo de instruções que o eMessage armazena no cache PrepareStatement por conexão com as tabelas de sistema. A configuração de poolMaxStatements como zero (0) desativa o armazenamento em cache da instrução.

Valor Padrão

0

Valores válidos

Um número inteiro igual ou maior que 0.

tempo de espera

Descrição

O número de segundos por que o eMessage mantém uma conexão com o banco de dados inativa antes de ele eliminar a conexão.

Se `poolIdleTestPeriod` for maior que 0, o eMessage testa todas as conexões inativas, agrupadas, menos as não verificadas, a cada `timeout` número de segundos.

Se `poolIdleTestPeriod` for maior que `timeout`, as conexões inativas são descartadas.

Valor Padrão

100

Valores válidos

Um número inteiro igual ou maior que 0.

eMessage | partitions | partition[n] | recipientListUploader

Essa categoria de configuração contém uma propriedade opcional para o local de um script definido pelo usuário que é executado em resposta às ações ou ao status do Recipient List Uploader.

pathToTriggerScript

Descrição

É possível criar um script que aciona uma ação em resposta ao upload de uma lista de destinatários para o IBM EMM Hosted Services. Por exemplo, é possível criar um script para enviar um alerta de email para o designer da lista quando o upload da lista for concluído com sucesso.

Se você definir um valor para esta propriedade, o eMessage passará informações de status sobre o Recipient List Uploader para o local especificado. O eMessage não executará nenhuma ação se deixar essa propriedade em branco.

Valor Padrão

Nenhum valor padrão definido.

Valores válidos

Qualquer caminho de rede válido.

eMessage | Partições | Partição[n] | responseContactTracker

As propriedades nesta categoria especificam o comportamento para o Response and Contact Tracker (RCT). O RCT recupera e processa dados para contatos de email, distribuição de emails e respostas de destinatários como cliques em links e aberturas.

pauseCustomerPremisesTracking

Descrição

O eMessage armazena dados de contatos e respostas em uma fila no IBM EMM Hosted Services. Defina essa propriedade para instruir o RCT a parar temporariamente de recuperar dados do IBM EMM Hosted Services. Quando você retoma o rastreamento, o RCT faz download dos dados acumulados.

Valor Padrão

False

Valores válidos

True | False

waitTimeToCheckForDataAvailability

Descrição

O RCT periodicamente verifica se há novos dados que estão relacionados a contatos de email ou respostas de destinatários. Especifique com que frequência, em segundos, o RCT verifica se há novos dados no IBM EMM Hosted Services. O valor padrão é 300 segundos, ou a cada 5 minutos.

Valor Padrão

300

Valores válidos

Qualquer número inteiro maior que 1.

perfLogInterval

Descrição

Defina um valor para esta propriedade para especificar quão frequentemente o RTC registra estatísticas de desempenho em um arquivo de log. O valor inserido determina o número de lotes entre entradas de log.

Valor Padrão

10

Valores válidos

Um número inteiro maior que 0.

enableSeparatePartialResponseDataTracking

Descrição

Essa propriedade determina se o eMessage encaminha dados de resposta de email parciais para as tabelas de rastreamento em sua instalação local do eMessage.

O eMessage requer o ID da Instância de Envio de Correio e o Número de Sequência da Mensagem para atribuit adequadamente respostas de email. Ao ativar o rastreamento de dados de resposta parciais separados, o eMessage coloca as respostas incompletas em tabelas de rastreamento locais separadas onde você possa revisá-las ou processá-los posteriormente.

Valor Padrão

True

Valores válidos

True | False

Capítulo 7. Utilitários para eMessage

O eMessage fornece vários scripts que você usa para administrar as funções do eMessage.

É possível utilizar os utilitários de software descritos nesta seção para uma variedade de funções de inicialização e administração. Além dos utilitários de software utilizados com o IBM Marketing Platform, o IBM eMessage usa utilitários são específicos para o eMessage e são usados apenas para gerenciar componentes do eMessage.

Para obter mais informações sobre outros utilitários disponíveis para sua instalação do IBM EMM, consulte *IBM Marketing Platform Administrator's Guide*.

O script do RLU

Utilize o script do RLU para verificar o status do Recipient List Uploader (RLU).

Nota: Não é possível utilizar este script para iniciar ou parar o RLU. Utilize este script apenas para verificar o status da conexão entre o RLU e o IBM EMM Hosted Services.

O script RLU está em seu diretório inicial do IBM EMM em `eMessage > bin`. O diretório eMessage é um subdiretório no diretório Campaign.

Em ambientes UNIX ou Linux, execute o script como `rlu.sh`.

No Windows, execute o script a partir do prompt de comandos como `rlu.bat`.

Sintaxe

```
rlu -c | --check [-h]
```

Comandos

-c, --check

Verifica se o RLU está configurado corretamente e se está conectado ao IBM EMM Hosted Services.

Opções

-h, --help

Exibe a sintaxe para o script

Exemplo

Em um ambiente Linux, determine se o RLU está conectado ao IBM EMM Hosted Services.

```
rlu.sh --check
```

Dependendo do status do seu sistema, a saída desse comando poderá ser semelhante a esta amostra.

```
Configurando a Origem de Dados [systemTables]...
Testando a configuração para a partição partition1
Testando a conectividade para a partição partition1
Testando acessibilidade do usuário para a partição partition1
Concluído com sucesso. Carregador de lista configurado e conectividade testada
com sucesso para a partição partition1
```

Tarefas relacionadas:

"Testando upload para o IBM EMM Hosted Services" na página 39

O script RCT

Utilize o script RCT para executar ou parar o Response and Contact Tracker (RCT) ou para determinar se ele pode se conectar com sucesso ao ambiente de email hospedado no IBM EMM Hosted Services.

Esse script está localizado no diretório `bin` na instalação do eMessage.O diretório eMessage é um subdiretório no diretório Campaign.

Nos ambientes UNIX ou Linux, execute o script como `rct.sh.`

No Windows, execute o script a partir do prompt de comandos como `rct.bat`.

Sintaxe

```
rct [ start | stop | check ]
```

Comandos

start

Inicia o RCT

parar

Para o RCT

Opções

check

Verifique a capacidade do RCT se conectar ao IBM EMM Hosted Services.

Exemplos

- Para iniciar o RCT no Windows.

  `rct.bat start`
- Para parar o RCT no Windows.

  `rct.bat stop`
- Em um ambiente Linux, determine se o RCT pode se conectar ao IBM EMM Hosted Services.

  `rct.sh check`

Se o RCT pode se conectar ao IBM EMM Hosted Services, a saída desse comando poderá aparecer como segue.

```
C:/Unica/emessage/bin>rct check
Testando configuração e conectividade para a partição partition1
Bem-sucedido | Partição: partition1 - ID da Conta de Serviços Hospedados:
asm_admin
```

Tarefas relacionadas:

"Incluindo o Response and Contact Tracker como um serviço" na página 35

"Testando download a partir do IBM EMM Hosted Services" na página 39

O script MKService_rct

Use esse script para incluir ou remover o Response and Contact Tracker (RCT) como um serviço. Incluir o RCT como um serviço reinicia o RCT sempre que o sistema operacional do computador no qual você instalou o RCT for reiniciado. Remover o RCT como um serviço evita que o RCT reinicie automaticamente.

Esse script está localizado no diretório `bin` na instalação do eMessage.

Nos ambientes do UNIX ou Linux, execute `MKService_rct.sh.` com um usuário que possua permissões de raiz ou permissões para criar processos daemon.

No Windows, execute o script a partir do prompt de comandos como `MKService_rct.bat`.

Sintaxe

```
MKService_rct -install
```

```
MKService_rct -remove
```

Comandos

-install

Inclua o RCT como um serviço

-remove

Remova o serviço RCT

Exemplos

- Para incluir o RCT como um serviço Windows.

  ```
  MKService_rct.bat -install
  ```

- Para remover o serviço RCT em UNIX ou Linux.

  ```
  MKService_rct.sh -remove
  ```

Conceitos relacionados:

"Sobre como iniciar o RCT automaticamente como um serviço" na página 34

Tarefas relacionadas:

"Incluindo o Response and Contact Tracker como um serviço" na página 35

O utilitário configTool

As propriedades e os valores na página Configuração são armazenados nas tabelas de sistema do Marketing Platform. O utilitário `configTool` importa e exporta definições de configuração para e a partir das tabelas de sistema do Marketing Platform.

Quando utilizar configTool

Talvez você deseje usar `configTool` pelas razões a seguir.

- Para importar modelos de partição e de origem de dados fornecidos com o Campaign, que podem então ser modificados e duplicados usando a página de Configuração.
- Registrar (propriedades de configuração de importação para) produtos do IBM EMM, se o instalador do produto não conseguir incluir as propriedades no banco de dados automaticamente.
- Para exportar uma versão XML das definições de configuração para backup ou para importação para uma instalação diferente do IBM EMM.
- Para excluir as categorias que não possuem o link **Excluir Categoria**. Isso é feito ao usar `configTool` para exportar sua configuração, em seguida, excluir manualmente o XML que cria a categoria e usar o `configTool` para importar o XML editado.

Importante: Esse utilitário modifica as tabelas `usm_configuration` e `usm_configuration_values` no banco de dados da tabela de sistema Marketing Platform, o qual contém as propriedades de configuração e seus valores. Para melhores resultados, crie cópias de backup destas tabelas ou exporte sua configuração existente usando `configTool` e faça backup do arquivo resultante para que você tenha uma maneira de restaurar sua configuração se cometer um erro ao usar `configTool` para importação.

Nomes de produtos válidos

O utilitário `configTool` usa nomes de produtos como parâmetros com os comandos que registram e cancelam o registro de produtos, conforme descrito posteriormente nesta seção. Com a liberação 8.0.0 do IBM EMM, muitos nomes dos produtos foram alterados. Entretanto, os nomes reconhecidos pelo `configTool` não foram alterados. Os nomes válidos dos produtos a serem usados com o `configTool` estão listados abaixo, juntamente com os nomes atuais dos produtos.

Nome do Produto	Nome usado no configTool
Marketing Platform	`Gerenciador`
Campaign	`Campanha`
Distributed Marketing	`Colaborar`
eMessage	`emessage`
Interact	`interagir`
Contact Optimization	`Otimizar`
Marketing Operations	`Planejar`
CustomerInsight	`Insight`
Digital Analytics for On Premises	`NetInsight`

Nome do Produto	Nome usado no configTool
PredictiveInsight	`Modelo`
Leads	`Lideranças`

Sintaxe

`configTool -d -p "*elementPath*" [-o]`

`configTool -i -p "*parent ElementPath*" -f *importFile* [-o]`

`configTool -x -p "*elementPath*" -f *exportFile*`

`configTool -r *productName* -f *registrationFile* [-o]`

`configTool -u *productName*`

Comandos

-d -p "*elementPath*"

Exclua as propriedades de configuração e suas definições, especificando um caminho na hierarquia de propriedades de configuração.

O caminho do elemento deve usar os nomes internos de categorias e de propriedades, o que é possível obter acessando a página Configuração, selecionando a categoria ou a propriedade desejada e examinando o caminho exibido nos parênteses na área de janela à direita. Delimite um caminho na hierarquia de propriedade de configuração usando o caractere | e coloque o caminho entre aspas duplas.

Note o seguinte.

- Apenas categorias e propriedades dentro de um aplicativo podem ser excluídas usando esse comando, e não os aplicativos inteiros. Use o comando `-u` para cancelar o registro de um aplicativo inteiro.
- Para excluir as categorias que não têm o link **Excluir Categoria** na página Configuração, use a opção `-o`.

-i -p "*parentElementPath*" -f *importFile*

Importe as propriedades de configuração e suas configurações a partir de um arquivo XML especificado.

Para importar, especifique um caminho para o elemento-pai sob o qual você deseja importar suas categorias. O utilitário `configTool` importa as propriedades *sob* a categoria que você especifica no caminho.

É possível incluir categorias em qualquer nível abaixo do nível superior, mas não é possível incluir uma categoria no mesmo nível que o da categoria superior.

O caminho do elemento-pai deve usar os nomes internos de categorias e propriedades, os quais podem ser obtidos na página Configuração, selecionando a categoria ou propriedade desejada, e consultando o caminho exibido entre

parênteses na área de janela à direita. Delimite um caminho na hierarquia de propriedade de configuração usando o caractere | e coloque o caminho entre aspas duplas.

É possível especificar um local do arquivo de importação relativo ao diretório `tools/bin` ou é possível especificar um caminho do diretório completo. Se especificar um caminho relativo ou nenhum caminho, `configTool` primeiro procurará o arquivo relativo ao diretório `tools/bin`.

Por padrão, esse comando não substitui uma categoria existente, mas é possível usar a opção `-o` para forçar uma substituição.

-x -p "*elementPath*" -f *exportFile*

Exporte as propriedades de configuração e suas configurações para um arquivo XML com um nome especificado.

É possível exportar todas as propriedades de configuração ou limitar a exportação a uma categoria específica especificando um caminho na hierarquia de propriedades de configuração.

O caminho do elemento deve usar os nomes internos de categorias e de propriedades, o que é possível obter acessando a página Configuração, selecionando a categoria ou a propriedade desejada e examinando o caminho exibido nos parênteses na área de janela à direita. Delimite um caminho na hierarquia de propriedade de configuração usando o caractere | e coloque o caminho entre aspas duplas.

É possível especificar um local do arquivo de exportação relativo ao diretório atual ou é possível especificar um caminho do diretório completo. Se a especificação de arquivo não contiver um separador (/ no Unix, / ou \ no Windows), o `configTool` gravará o arquivo para o diretório `tools/bin` na sua instalação do Marketing Platform. Se você não fornecer a extensão `xml`, o `configTool` a incluirá.

-r *productName* -f *registrationFile*

Registre o aplicativo. O local do arquivo de registro pode ser relativo ao diretório `tools/bin` ou pode ser um caminho completo. Por padrão, esse comando não sobrescreve uma configuração existente, mas é possível usar a opção `-o` para forçar uma sobrescrição. O parâmetro *`productName`* deve ser um daqueles listados acima.

Note o seguinte.

- Quando a opção `-r` é usada, o arquivo de registro deve ter `<application>` como a primeira tag no XML.

  Outros arquivos podem ser fornecidos com o produto e podem ser usados para inserir propriedades de configuração do banco de dados do Marketing Platform. Para esses arquivos, use a opção `-i`. Somente o arquivo que possui a tag `<application>` como a primeira tag poderá ser usado com a opção `-r`.
- O arquivo de registro para o Marketing Platform é chamado `Manager_config.xml`, e a primeira tag é `<Suite>`. Para registrar esse arquivo em uma nova instalação, use o utilitário `populateDb`, ou execute novamente o instalador do Marketing Platform conforme descrito no *Guia de Instalação do IBM Marketing Platform*.

- Após a instalação inicial, para registrar novamente outros produtos além do Marketing Platform, use o `configTool` com a opção `-r` e `-o` para substituir as propriedades existentes.

-u *productName*

Cancele o registro de um aplicativo especificado por *productName* . Não é necessário incluir um caminho na categoria do produto; o nome do produto é suficiente. O parâmetro *productName* deve ser um daqueles listados acima. Isso remove todas as propriedades e definições de configuração para o produto.

Opções

-o

Quando usado com `-i` ou `-r`, substitui uma categoria ou registro de produto existente (nó).

Quando usado com a opção `-d`, permite excluir uma categoria (nó) que não possui o link **Excluir Categoria** na página de Configuração.

Exemplos

- Importar definições de configuração de um arquivo denominado `Product_config.xml` localizado no diretório `conf` sob a instalação do Marketing Platform.

  ```
  configTool -i -p "Affinium" -f Product_config.xml
  ```

- Importe um dos modelos de origem de dados do Campaign fornecidos na partição padrão do Campaign, a partition1. O exemplo assume que você colocou o modelo de origem de dados Oracle, `OracleTemplate.xml`, no diretório `tools/bin` na instalação do Marketing Platform.

  ```
  configTool -i -p "Affinium|Campaign|partitions|partition1|dataSources" -f
  OracleTemplate.xml
  ```

- Exportar todas as definições de configuração para um arquivo denominado `myConfig.xml` localizado no diretório `D:\backups`.

  ```
  configTool -x -f D:\backups\myConfig.xml
  ```

- Exporte uma partição do Campaign existente (complete com entradas de origem de dados), salve-a para um arquivo chamado `partitionTemplate.xml` e armazene-a no diretório padrão `tools/bin` na instalação do Marketing Platform.

  ```
  configTool -x -p "Affinium|Campaign|partitions|partition1" -f
  partitionTemplate.xml
  ```

- Registrar manualmente um aplicativo denominado productName, usando um arquivo denominado `app_config.xml` localizado no diretório `tools/bin` padrão sob a instalação do Marketing Platform e forçá-lo a sobrescrever um registro existente deste aplicativo.

  ```
  configTool -r product Name -f app_config.xml -o
  ```

- Cancelar registro de um aplicativo denominado productName.

  ```
  configTool -u productName
  ```

Fazendo backup de definições de configuração

Para fazer backup das definições de configuração do eMessagee do Campaign, utilize o utilitário `configTool` para exportar uma cópia de definições de configuração atuais a partir do IBM Marketing Platform em um arquivo.

Sobre Esta Tarefa

Para obter detalhes sobre como utilizar o utilitário `configTool`, incluindo a explicação da sintaxe e parâmetros, consulte “O utilitário configTool” na página 60.

Executar o backup com `configTool` exporta todas as configurações de propriedade atuais na categoria `emessage` nas configurações. Ao executar o backup, especifique um nome de arquivo para o arquivo`.xml` exportado e anote o local onde ele foi salvo.

Por exemplo,

No Windows:

```
configTool.bat -x -p "emessage" -f emessageProperties.xml
```

No UNIX ou Linux:

```
configTool.sh -x -p "emessage" -f emessageProperties.xml
```

Por padrão, o arquivo `.xml` é exportado para o diretório `*MANAGER_HOME*/xml`.

Capítulo 8. Sobre a Resolução de Problemas do eMessage

O IBM eMessage fornece várias ferramentas e técnicas que podem ser utilizadas para investigar problemas relacionados às suas instalações do Campaign e do eMessage.

Arquivos de log para o eMessage

O IBM EMM fornece vários arquivos de log que podem ser revisados para monitorar sua instalação do eMessage e investigar problemas.

Arquivo de log do eMessage

Este log contém os seguintes tipos de informações sobre as informações transferidas por download a partir do IBM EMM Hosted Services.

- informações gerais de correspondência
- ID da instância de correspondência
- dados de clique de link
- dados para email devolvido

Localizado no diretório `logs` em sua instalação do eMessage.

Arquivos temporários do eMessage

Este diretório contém os dados que estão sendo transferidos por upload.

Localizado no diretório `temp` na sua instalação do eMessage.

Arquivos de log do Campaign

É possível revisar os arquivos de log nos seguintes locais para obter informações relacionadas à atividade de correspondência no Campaign.

- `Campaign\partitions\<partitionN>\logs`

  Vários arquivos de log relacionados com execuções do fluxograma, incluindo as entradas de log de qualquer processo do eMessage contido no fluxograma.
- `Campaign\logs`

  Esse diretório contém `campaignweb.log` que contém informações sobre a atividade de upload executada pelo Recipient List Uploader.

Utilizando log4j com eMessage

O eMessage usa o utilitário Apache log4j para o registro de configuração, depuração e informações de erro relacionados ao Response and Contact Tracker (RCT) e ao Recipient List Uploader (RLU).

Para obter informações sobre como alterar as configurações de log do sistema, consulte:

- Os comentários no arquivo log4j.properties.
- A documentação log4j no site da web apache: http://logging.apache.org/log4j/1.2/manual.html

Utilizando log4j com o Recipient List Uploader

Quando executar o utilitário RLU a partir da linha de comandos, ele utiliza as configurações do criador de logs padrão. Para alterar essas definições, modifique o arquivo `emsg_rlu_log4j.properties`. No diretório `conf` em sua instalação do eMessage, copie `example_emsg_log4j.properties` para `emsg_rlu_log4j.properties`. Modifique `emsg_rlu_log4j.properties` conforme instruído pelos comentários nesse arquivo.

Quando o RLU é chamado automaticamente por um fluxograma, ele utiliza a criação de log do aplicativo da web do Campaign que é configurado no `campaign_log4j.properties` em seu diretório de instalação do Campaign.

Utilizando log4j com o Response and Contact Tracker

Ao executar o utilitário Response and Contact Tracker (RCT), ele utiliza as configurações do criador de logs padrão. Para alterar essas configurações, modifique o arquivo `emsg_rct_log4j.properties`. No diretório `conf` em seu diretório de instalação do eMessage, copie `example_emsg_log4j.properties` para `emsg_rct_log4j.properties`. Modifique `emsg_rct_log4j.properties` conforme instruído pelos comentários nesse arquivo.

Capítulo 9. Gerenciamento de acesso do usuário aos recursos do sistema de mensagens

O Campaign e o eMessage usam funções e permissões fornecidas pelo IBM Marketing Platform para controlar o acesso do usuário a recursos do sistema de mensagens no eMessage e Campaign. Você deve ter permissões no IBM Marketing Platform e Campaign para fazer as mudanças necessárias. Você também deve estar familiarizado com o modo de configurar funções e permissões no Marketing Platform e como definir políticas de segurança para o Campaign.

Para realizar campanhas de marketing por email, os comerciantes por email acessam os recursos de correspondência do eMessage no IBM Campaign.

Para criar comunicações personalizadas e páginas de entrada hospedadas, os comerciantes trabalham com os recursos e com o conteúdo no Editor de Documentos do eMessage.

Para obter informações gerais sobre como configurar funções, permissões e políticas, consulte as seções do *IBM Marketing Platform Administrator's Guide* que descrevem como gerenciar a segurança no IBM Marketing Platform e IBM Campaign.

Conceitos relacionados:

"Designação de função e de política para acessar correspondência"

"Permissões de sistema de mensagens no Campaign" na página 70

"Permissões do sistema de mensagens para o eMessage" na página 75

Designação de função e de política para acessar correspondência

Para efetuar login no sistema IBM EMM, os comerciantes por email inserem um nome do usuário e senha do sistema. As permissões que são concedidas ao usuário do sistema determinam como o comerciante pode acessar os recursos de correspondência, comunicações personalizadas e conteúdo no eMessage e Campaign.

As permissões são associadas Às funções que são definidas no IBM Marketing Platform. Para controlar o acesso aos recursos de correspondência no Campaign, é possível definir funções dentro de uma ou mais políticas de segurança. Todos os usuários do sistema que acessam os recursos de correspondência, comunicações e conteúdo devem ser designados a uma função do eMessage na política de segurança do Campaign. Com a política, você aplica seletivamente permissões para recursos de correspondência no Campaign e para comunicações e conteúdo no Editor de Documentos do eMessage.

Os usuários que acessam os recursos de correspondência também devem ser designados às funções de usuário e administração do eMessage. Essas funções são separadas das funções do eMessage disponíveis nas políticas de segurança do Campaign.

Conceitos relacionados:

"Permissões do sistema de mensagens para o eMessage" na página 75

Capítulo 9, “Gerenciamento de acesso do usuário aos recursos do sistema de mensagens”, na página 67
“Sobre funções e permissões no Marketing Platform e o Campaign”
“Permissões de sistema de mensagens no Campaign” na página 70

Sobre funções e permissões no Marketing Platform e o Campaign

As funções no Marketing Platform e no Campaign são uma coleta configurável de permissões. Para cada função no Marketing Platform e no Campaign, é possível especificar permissões que controlam o acesso ao aplicativo. É possível utilizar as funções padrão ou criar novas funções. O conjunto de permissões disponíveis é definido pelo sistema; não é possível criar uma nova permissão.

Sobre designação de função

Geralmente deve-se conceder aos usuários funções com permissões que refletem as funções que os usuários executam na organização quando usam o IBM EMM. É possível designar funções para um grupo ou para um usuário individual. A vantagem de designar funções por grupo é a possibilidade de designar uma combinação de funções para o grupo e, quando desejar alterar essa combinação mais tarde, fazer isso em um local e não diversas vezes para diversos usuários. Ao designar funções por grupo, você inclui e remove usuários dos grupos para controlar o acesso do usuário.

Como o sistema avalia as funções

Se um usuário tiver diversas funções, o sistema avaliará as permissões de todas essas funções juntas. Em seguida, a capacidade de executar uma função em um determinado objeto é concedida ou negada com base nas permissões agregadas de todas as funções. No caso do Campaign, a capacidade de executar uma função em um determinado objeto é concedida ou negada com base na política de segurança do objeto.

Conceitos relacionados:

“Designação de função e de política para acessar correspondência” na página 67
“Funções do eMessage na Política Global” na página 70

Sobre as políticas de segurança

As políticas de segurança são os "livros de regras" que regem a segurança no Campaign; eles são consultados cada vez que um usuário executa uma ação no aplicativo. As políticas de segurança são criadas por partição (não há compartilhamento de políticas de segurança por meio de partições). Uma partição no Campaign pode ter várias políticas de segurança.

Uma política de segurança consiste de várias funções que são definidas. Cada função contém um conjunto de permissões que determinam as ações que os usuários podem executar e os objetos que eles podem acessar. É possível designar usuários a uma função diretamente ou designar grupos para uma função (os usuários nesses grupos são designados à função).

Ao criar um objeto como uma campanha ou oferta na pasta de nível superior, uma política de segurança é aplicada ao objeto. Além disso, ao criar uma pasta de nível superior, uma política de segurança é aplicada à pasta e todos os objetos ou subpastas criados nessa pasta herdam a política de segurança que foi aplicada na pasta.

Aplicar políticas de segurança a objetos ou pastas permite separar os objetos no Campaign para uso por diferentes grupos de usuários. Por exemplo, é possível configurar suas políticas de segurança para que os usuários pertencentes a uma política não possam acessar ou nem mesmo visualizar os objetos que estiverem associados a outras políticas.

É possível criar suas próprias políticas de segurança ou utilizar a política de segurança global padrão incluída com o Campaign.

A política de segurança global

O Campaign inclui uma política de segurança global padrão que pode ser utilizada no estado em que se encontra ou modificada para se adequar às necessidades de sua organização. Se optar por não criar as suas próprias políticas de segurança, a política de segurança global será aplicada, por padrão, nos objetos que forem criados no Campaign.

É possível utilizar a política global, além de suas próprias políticas, ou utilizar suas próprias políticas exclusivamente. Não é possível excluir a política global, mesmo se ela não estiver em uso.

Quaisquer políticas de segurança que forem criadas existem sob a política de segurança global. Na política global, é possível criar uma política de segurança separada para os funcionários de cada divisão em sua organização.

A política de segurança global contém seis funções predefinidas e é possível incluir funções na política global, se necessário. Não é possível excluir as funções predefinidas, mas é possível modificar suas permissões.

As funções predefinidas são:

- **Proprietário da Pasta –** Todas as permissões ativadas
- **Proprietário do Objeto –** Todas as permissões ativadas
- **Administração –** Todas as permissões ativadas. O usuário padrão `asm_admin` é designado a essa função.
- **Execução –** Todas as permissões ativadas
- **Design –** Permissões de leitura e gravação na maioria dos objetos. Não é possível planejar fluxogramas ou sessões.
- **Revisão –** Permissões somente leitura

A política de segurança global se aplica a todos os usuários por meio das funções de proprietário e de proprietário da pasta, incluindo os usuários que não foram designados a nenhuma outra função específica na política global. Como a política global sempre se aplica, ela pode ser utilizada, por exemplo, para negar globalmente as permissões de uma função.

Conceitos relacionados:

"Funções do eMessage na Política Global" na página 70

Funções do eMessage na Política Global

Além das funções predefinidas do Campaign, a Política global inclui várias funções específicas ao eMessage.

A Política global inclui as funções a seguir do eMessage.

- **eMsg_admin** - Permite acesso a todos os recursos de correspondência, todo o conteúdo e todos os documentos.
- **eMsg_execute –** Permite acesso a todos os recursos de correspondência, todo o conteúdo e todos os documentos.
- **eMsg_design –** Permite acesso a todo o conteúdo, todos os documentos e à maioria dos recursos de correspondência. Entretanto, não é concedida explicitamente permissão para enviar correspondências de produção.
- **eMsg_review –** Permite apenas visualizar o conteúdo e os documentos e possui permissões limitadas para trabalhar com as correspondências. Não é concedida explicitamente permissão para incluir, editar ou excluir correspondências. É permitido visualizar e enviar correspondências de teste e de produção.

Nota: O eMessage não suporta as funções Proprietário e Proprietário de Pasta que são criadas por padrão para o Campaign.

Conceitos relacionados:

"Sobre funções e permissões no Marketing Platform e o Campaign" na página 68

"A política de segurança global" na página 69

"Permissões para Correios em Campanha" na página 73

"Permissões para a Categoria Ativos Digitais" na página 73

"Permissões para a Categoria de Documentos" na página 74

Permissões de sistema de mensagens no Campaign

O Campaign controla o acesso do usuário aos recursos de correspondência ao ativar ou desativar permissões específicas que são definidas em funções que são designadas para um usuário ou grupo. Essas funções são associadas a uma ou mais políticas de segurança. É possível definir várias políticas de segurança do Campaign e designar diversas funções para cada política. Cada combinação de política e funções pode definir um conjunto específico de permissões.

Para obter mais informações sobre como gerenciar permissões de segurança, incluindo cenários de segurança de amostra, consulte o *IBM Campaign Administrator's Guide*.

Em Funções e Permissões para o IBM Marketing Platform, designe permissões do usuário para recursos e conteúdo de correspondência na seção Campaign da seguinte forma:

1. Defina funções de usuário.

   As funções do usuário definidas pelo sistema para o eMessage são criadas, por padrão, na Política Global.

   Também é possível definir funções customizadas e incluí-las na Política Global ou em outras políticas que você definir.
2. Defina políticas de segurança e inclua funções do usuário nas políticas.

   A política global é definida por padrão. É possível definir políticas adicionais para o Campaign.

3. Defina permissões específicas para cada função em cada política.

   É possível definir políticas adicionais e funções customizadas com vários conjuntos de permissões para maior controle sobre o acesso a recursos de correspondência no no Editor de documentos do Campaign e do eMessage.

As mudanças em permissões, funções e políticas são aplicadas quando o usuário efetua login no IBM EMM. Após designar ou alterar permissões de correspondência para um usuário, o usuário deverá efetuar logout e, em seguida, login novamente para que as mudanças sejam observadas.

Conceitos relacionados:

Capítulo 9, “Gerenciamento de acesso do usuário aos recursos do sistema de mensagens”, na página 67

“Designação de função e de política para acessar correspondência” na página 67

Criando funções e permissões disponíveis

Dependendo de sua instalação do IBM Marketing Platform, os controles administrativos que são necessários para definir e aplicar funções e permissões podem não ficar imediatamente visíveis. É possível tornar os controles necessários visíveis ao acessar o Editor de Documentos do eMessage ou uma correspondência no Campaign.

Sobre Esta Tarefa

Execute o procedimento a seguir se você não vir todas as seguintes permissões na Política Global Campaign.

- Permissões para correspondências na categoria Campanhas
- Permissões para a Biblioteca de Conteúdo na categoria de Ativos Digitais
- Permissões para documentos do eMessage na categoria Documentos

Procedimento

1. Efetue login noIBM EMM.

   Se tiver diversos usuários configurados, efetue login como um usuário com as permissões mais limitadas. Por exemplo, efetue login como um usuário apenas com as permissões de Visualização.
2. Navegue até **Campanha** > **Documentos do eMessage** para acessar o Editor de documentos.

   Aguarde até o Editor de Documentos concluir o carregamento.
3. Navegue até **Configurações** > **Funções e permissões do usuário** > **Campanha** > **partição [n]** > **Política global**

   Quando solicitado, confirme se deseja sair do Editor de Documentos ao sair da página.
4. Clique em **Incluir Funções e Designar Permissões**. As funções do eMessage a seguir estão visíveis.
   - eMsg_admin
   - eMsg_execute
   - eMsg_design
   - eMsg_review
5. Clique em **Salvar e Editar Permissões**.

As permissões de correspondência estão visíveis nas categorias Campainhas, Ativos Digitais, e Documentos.

Para obter mais informações sobre as permissões específicas que estão disponíveis, consulte os seguintes tópicos.

Conceitos relacionados:

"Permissões para Correios em Campanha" na página 73

"Permissões para a Categoria Ativos Digitais" na página 73

"Permissões para a Categoria de Documentos" na página 74

Como o Campaign avalia as permissões

Quando um usuário executa uma tarefa ou tenta acessar um objeto, o Campaign executa as seguintes etapas:

1. Identifica todos os grupos e funções aos quais esse usuário pertence dentro da política de segurança global. Um usuário pode pertencer a uma, muitas ou nenhuma função. Um usuário pertencerá à função de proprietário se ele possuir um objeto e pertencerá à função de proprietário da pasta se ele possuir a pasta na qual um objeto reside. Um usuário pertencerá a outras funções apenas se ele tiver sido designado especificamente para essa função (seja diretamente ou porque eles pertencem a um grupo designado a essa função).
2. Identifica se o objeto que está sendo acessado foi designado a uma política definida por customização, se alguma existir. Se sim, então o sistema identificará todos os grupos e funções aos quais o usuário pertence dentro desta política customizada.
3. Agrega as permissões para todas as funções às quais o usuário pertence com base nos resultados das etapas 1 e 2. Utilizando essa função composta, o sistema avaliará as permissões para a ação da seguinte forma:
   a. Se quaisquer funções tiverem a permissão **Negada** para esta ação, o usuário não terá permissão para executar essa ação.
   b. Se nenhuma função tiver a permissão **Negada** para esta ação, ele verificará a permissão para determinar se alguma função tem a permissão **Concedida** para essa ação. Se tiver, o usuário terá permissão para executar a ação.
   c. Se nem a nem b for true, o usuário terá a permissão negada.

Definição de estados de permissão

Para cada função, é possível especificar qual das permissões predefinidas são concedidas, não são concedidas ou são negadas. Estes estados têm os seguintes significados.

- **Concedida** - indicado com um visto verde . Concede explicitamente permissão para desempenhar esta função específica, desde que nenhuma das outras funções do usuário tenha permissão negada explicitamente.
- **Negado –** Indicado com um "X" vermelho . Nega explicitamente a permissão para desempenhar esta função específica, independentemente de quaisquer outras funções do usuário que podem conceder a permissão.
- **Não Concedido –** Indicado com um "X" cinza sombreado . Não concede nem nega explicitamente permissão para executar uma função específica. Se essa permissão não for concedida explicitamente por nenhuma das funções do usuário, o usuário não terá permissão para executar esta função.

Permissões para Correios em Campanha

No Campaign, você cria, configura, executa e monitora os correios do eMessage com controles nas guias de correio do eMessage. Você gerencia cada correio em uma guia separada.

As permissões a seguir controlam o acesso de usuário às guias de correio do eMessage. Elas estão na categoria de **Campanhas**.

Permissão	Descrição
Visualizar Correios	Permite que um usuário visualize uma guia de correio do eMessage em uma campanha. O usuário não pode editar ou alterar o correio.
Editar Correios	Permite que um usuário configure ou altere uma guia de correio do eMessage em uma campanha.
Excluir Correios	Permite que um usuário remova um correio do eMessage de uma campanha.
Incluir Correios	Permite que um usuário crie um correio em uma campanha.
Enviar correio de produção	Permite que o usuário inicie uma execução de produção do correio, ative um correio para email transacional ou programe uma execução de correio em produção. Correios de produção podem incluir muitas mensagens. As mensagens de email são enviadas para todas as pessoas identificadas como um destinatário de produção na lista de destinatários que é associada à correspondência.
Executar execução de teste	Permite ao usuário iniciar uma execução de teste do correio. Correios de teste geralmente envolvem poucas mensagens. Durante uma execução de teste, uma mensagem de email é enviada para cada endereço identificado como um destinatário do teste na lista de destinatários que é associada à correspondência.

Conceitos relacionados:

"Funções do eMessage na Política Global" na página 70

Tarefas relacionadas:

"Criando funções e permissões disponíveis" na página 71

Permissões para a Categoria Ativos Digitais

O permissões de Ativos Digitais controlam o acesso de usuário a elementos de conteúdo na Biblioteca de Conteúdo do eMessage e a pastas e subpastas nas quais eles estão armazenados.

A Biblioteca de Conteúdo é um repositório para elementos de conteúdo (também chamados de ativos digitais) que são usados em comunicações que os usuários criam no Editor de Documentos do eMessage.

Permissões	Descrição
Visualizar os ativos digitais do eMessage	Permite que um usuário abra os elementos de conteúdo para visualizar propriedades e visualizar o conteúdo que pode ser incluído em uma comunicação personalizada.

Permissões	Descrição
Criar novos ativos digitais na biblioteca de conteúdo do eMessage	Permite a um usuário criar um elemento de conteúdo e incluí-lo na Biblioteca de Conteúdo.
Editar ativos digitais existentes na biblioteca de conteúdo do eMessage	Permite a um usuário abrir e editar elementos de conteúdo existentes.
Excluir ativos digitais da biblioteca de conteúdo do eMessage	Permite a um usuário remover um elemento de conteúdo da Biblioteca de Conteúdo.
Mover ativos digitais de uma pasta para outra	Permite a um usuário mover os elementos de conteúdo dentro da Biblioteca de Conteúdo. Mover um elemento de conteúdo requer designar essa permissão às pastas de origem e de destino.

Conceitos relacionados:

"Funções do eMessage na Política Global" na página 70

Tarefas relacionadas:

"Criando funções e permissões disponíveis" na página 71

Permissões para a Categoria de Documentos

As permissões na categoria **Documentos** controlam o acesso de usuário para criar, editar e gerenciar comunicações personalizadas no Editor de Documentos do eMessage.

Permissões	Descrição
Visualizar documentos do eMessage	Permite que um usuário visualize um documento que é usado para criar um email ou página de entrada do host.
Criar novos documentos do eMessage	Permite ao usuário criar uma nova comunicação personalizada.
Editar documentos existentes do eMessage	Permite ao usuário alterar uma comunicação personalizada existente.
Excluir documentos do eMessage	Permite ao usuário remover uma comunicação personalizada.
Publicar documento do eMessage, tornando o conteúdo disponível na Internet pública.	Permite ao usuário publicar uma comunicação personalizada. A publicação de uma comunicação torna o documento e todo o seu conteúdo disponível para uso em um correio do eMessage.
Copie os documentos do eMessage de uma pasta para outra.	Permite a um usuário copiar uma comunicação personalizada entre pastas na Biblioteca de Conteúdo. A cópia de uma comunicação requer designar essa permissão para pastas de origem e de destino.

Permissões	Descrição
Mover documentos do eMessage de uma pasta para outra.	Permite ao usuário mover uma comunicação personalizada de uma pasta para outra pasta na Biblioteca de Conteúdo. A movimentação de uma comunicação requer designar essa permissão para pastas de origem e de destino.

Conceitos relacionados:

"Funções do eMessage na Política Global" na página 70

Tarefas relacionadas:

"Criando funções e permissões disponíveis" na página 71

Permissões para a categoria de Administração de Email

As permissões na categoria **Administração de Email** da Política Global do Campaign fornecem aos administradores do eMessage acesso às configurações que controlam quais domínios de email estão disponibilizados para usuários do eMessage.

As permissões permitem que o administrador restrinja a lista de domínios de email que o usuário pode selecionar como um domínio **De:** em uma comunicação por email que é criada no Editor de Documentos do eMessage.

Para poder controlar a lista de domínios de email disponíveis para os usuários do eMessage, um administrador deverá ter permissão para Configurar Domínios. A permissão para configurar domínios permite que um usuário administrador acesse a seção Configurações da Política da janela Configurações do eMessage. A seção Configurações de Política não é exibida, a menos que a permissão Configurar Domínios seja concedida explicitamente ao administrador como parte da Política Geral do Campaign.

Permissões	Descrição
Configurar domínios	Controla o acesso à seção Configurações da Política da página Configurações do eMessage. Se à função de administrador não for concedida a permissão para configurar domínios de email, o administrador não poderá ver a seção Configurações de Política.

Permissões do sistema de mensagens para o eMessage

O IBM eMessage controla o acesso a recursos de correspondência fora da guia Correspondência no Campaign por meio das funções de segurança predefinidas a seguir.

- `eMessage_admin`
- `eMessage_user`

Os usuários devem ter ambas as funções para ter acesso aos recursos de correio do eMessage.

Conceitos relacionados:

"Designação de função e de política para acessar correspondência" na página 67

Capítulo 9, "Gerenciamento de acesso do usuário aos recursos do sistema de mensagens", na página 67

Tarefas relacionadas:

"Designando funções do eMessage"

Designando funções do eMessage

Para fornecer a um usuário o acesso total aos recursos de correspondência do eMessage, designe as funções predefinidas do eMessage ao usuário.

Procedimento

1. No IBM Marketing Platform, navegue até `Configurações > Funções do usuário & Permissões > eMessage > partição [n] > eMessage_admin`.
2. Clique em **Designar Usuários**.
3. Selecione o usuário na lista de usuários disponíveis. Clique em **Incluir** para designar a função para o usuário.
4. Repita as etapas 1 a 3 para a função `eMessage_user`.
5. Salve as alterações.

Conceitos relacionados:

"Permissões do sistema de mensagens para o eMessage" na página 75

Controlando domínios de email e domínios de link curto

Mediante solicitação, o IBM configura um ou mais domínios de email para sua conta de email hospedada. IBM também pode atribuir domínios que os comerciantes usam para criar links curtos em diversos tipos de mensagens. Os administradores do sistema com permissões apropriadas controlam os domínios do sistema de mensagens que ficam disponíveis para os comerciantes.

Sobre Esta Tarefa

Dependendo de seus requisitos de negócios, pode ser desejável restringir a lista de domínios do sistema de mensagens que estão disponíveis para comerciantes específicos. Os administradores do eMessage restringem a lista de domínios disponíveis por meio de políticas de segurança que são aplicadas a pastas no Editor de Documentos. A capacidade dos comerciantes para criar e editar comunicações de email depende da política de segurança que é aplicada à pasta que contém a comunicação.

Os administradores do eMessage com as permissões apropriadas podem controlar a lista de domínios de email que os usuários do eMessage podem utilizar como o domínio **De:** em comunicações de email. Os administradores também podem controlar a lista de domínios de link curto que é apresentado para comerciantes quando eles configuram as comunicações que usam links curtos. Por exemplo, você pode especificar quais domínios de link curto ficam disponíveis quando comerciantes incluem um link de compartilhamento social para mensagens de marketing.

Os administradores do eMessage usam a página Configurações de política para conceder permissões para usar domínios específicos do sistema de mensagem. O acesso à página Configurações da política é controlado pelas permissões Administração de email que são concedidas através da Política global da

campanha. Somente os administradores com as permissões apropriadas podem restringir o acesso aos domínios de email por meio da página Configurações de Política.

Procedimento

1. No menu **Configurações**, selecione Configurações do eMessage. Se tiver as permissões administrativas apropriadas, a seção Configurações de Política será exibida na página Configurações do eMessage.
2. Clique em **Exibir uma lista de políticas e suas configurações**. Uma lista de políticas de segurança que são configuradas para a sua instalação do eMessage é exibida.
3. Clique em uma política de segurança que esteja associada ao usuário do sistema cujo acesso de domínio do sistema de mensagens você queira controlar.

   A seção Domínio exibe os domínios de email que são configurados para sua conta do sistema de mensagens hospedado.

   A seção Domínios de link curto exibe os domínios de link curto que são configurados para sua conta do sistema de mensagens hospedado.

   - Em uma das seções, clique em **Usar todos os domínios** para permitir que os usuários associados à política usem qualquer um dos domínios de email que o IBM configurou para sua conta de email hospedada.

     Essa opção é a padrão.
   - Clique em **Usar domínios específicos** para selecionar domínios específicos.

     Nota: Se selecionar **Usar domínios específicos**, deve-se atualizar as permissões de domínio quando você registrar um novo email ou domínio de link curto para sua conta do sistema de mensagem hospedada. O sistema não designa permissões para o novo domínio automaticamente.

Resultados

Para usuários associados à política de segurança, somente os domínios de email selecionados aparecem como uma opção para o endereço **De:** nas comunicações por email. Para comunicações que requerem links links curtos, os comerciantes podem escolher somente dos domínios de link curto específicos que você seleciona.

Depois de salvar as novas configurações, o Editor de Documentos atualiza as opções de domínio que ficam disponíveis aos comerciantes.

Para obter mais informações sobre como os comerciantes do eMessage criam e gerenciam comunicações, consulte o *IBM eMessage User's Guide*.

Manutenção de domínios de email hospedados

Para enviar emails, você deve registrar pelo menos um domínio de email com o IBM. Para melhorar a entrega de mensagens, o IBM trabalha com você para estabelecer e manter a reputação de email do domínio com os principais Provedores de Serviços da Internet (ISPs) em todo o mundo. É possível estabelecer vários domínios de email com IBM.

Ao configurar o cabeçalho em uma comunicação por email, o sistema preenche o endereço De com o domínio de email que você registrou com o IBM. Se estabelecer diversos domínios de email com o IBM, os domínios disponíveis serão exibidos em uma lista suspensa. Os administradores do sistema podem controlar os domínios de email que os comerciantes por email podem selecionar ou modificar.

É possível solicitar que o IBM inclua ou exclua os domínios de email estabelecidos para sua conta do sistema de mensagens hospedado. Depois que o IBM conclui a mudança, o sistema atualizará a lista de domínios de email disponíveis. A mudança é refletida na lista de domínios de email disponíveis na próxima vez que criar ou editar uma comunicação por email.

Nota: As mudanças de domínio de email para sua conta não atualizam comunicações de email criadas antes da solicitação de mudança. Para alterar o domínio de email para uma comunicação criada anteriormente, deve-se reabrir a comunicação por email e atualizar a seleção de domínio de email.

Para obter mais informações sobre como registrar um domínio de email com o IBM, consulte *Opções de nome de domínio do IBM Enterprise Marketing Management (EMM) para email.*

Para solicitar mudanças relacionadas aos seus domínios de email, entre em contato com os Serviços de Conta de Email em `eacctsvc@us.ibm.com`.

Configurando o endereço de remetente e os nomes de exibição padrão

Para cada domínio de email que você registrou com o IBM, é possível definir um endereço de email padrão e um nome fácil padrão. A combinação do endereço de email ou do nome fácil com o domínio de email aparece como o endereço De: para as mensagens de email que são enviadas.

Sobre Esta Tarefa

Os administradores podem configurar o remetente e os nomes de exibição padrão na página Configurações do Domínio. As configurações de domínio são parte da interface do eMessage Settings. O acesso à página Configurações de domínio é controlado pelas permissões de Administração de email concedidas por meio da Política global do Campaign. Somente os administradores com as permissões apropriadas podem restringir o acesso aos domínios de email por meio da página Configurações de Política.

Procedimento

1. Acesse **Configurações** > **Configurações do eMessage**. Na seção Configurações do Domínio, clique em **Exibir** na lista de configurações de domínio.

   A página Configurações Domínio lista os nomes de exibição e os endereços de email associados aos domínios de email que são registrados para sua conta de email hospedada. A lista inclui apenas os domínios que suas permissões de usuário permitem modificar.

   A coluna Padrão indica a combinação do nome de exibição, do endereço e do domínio que aparece como o endereço De padrão para novas comunicações de email.

2. Clique em **Editar** . A janela Editar Configurações de Domínio se abre.

   A coluna Nome do Domínio lista os domínios de email disponíveis. É possível fazer o seguinte para qualquer um dos domínios.

   - Na coluna Nome de Exibição De, insira um nome fácil para aparecer como o padrão para um domínio de email na lista.

- Na coluna Endereço De, insira a parte local do endereço de email a ser exibido como o padrão para um domínio de email na lista.

3. Opcionalmente, na coluna Padrão, selecione uma combinação de endereço de nome de exibição e o domínio a serem exibidos como o endereço De padrão para novas comunicações de email.

   Se não selecionar um padrão, o sistema usará o primeiro domínio na lista para criar o endereço De padrão para novas comunicações por email.
4. Salve as alterações.

Resultados

As novas configurações se aplicam a todas as comunicações de email novas que você criar. As configurações não alteram informações de endereço para comunicações de email criadas anteriormente. Para atualizar comunicações de email anteriores, deve-se reabrir e modificar cada comunicação.

Controlando o acesso à lista de mensagens enviadas

O eMessage fornece uma lista de mensagens que foram enviadas do seu ambiente do eMessage. Como a lista inclui links em configurações do sistema de mensagens, seus planos de segurança podem requerer que você restrinja o acesso à lista.

Sobre Esta Tarefa

A lista de mensagens é apresentada na página **Correspondências do eMessage**. Por padrão, todos os usuários no ambiente do Campaign e eMessage podem ver a lista de mensagens enviadas. Entretanto, ao ativar a restrição de acesso, é possível impedir que os usuários específicos vejam a opção de menu para abrir a página que contém a lista.

Restringir o acesso à lista de mensagens enviadas afeta todas as partições em sua instalação do Campaign. Se sua instalação do Campaign incluir diversas partições, você deve atualizar permissões do usuário separadamente em cada partição para conceder explicitamente ou negar a permissão para acessar a lista.

Controlar quem pode acessar a lista de mensagens enviadas requer uma série de tarefas para alterar permissões do usuário e a configuração do sistema.

Tarefa	Mais informações
Identifique os usuários que podem acessar a lista de mensagens. Em primeiro lugar, todos os usuários recebem acesso.	"Concedendo acesso à lista de mensagens enviadas" na página 80
Identifique os usuários que não têm permissão para acessar a lista de mensagens.	"Negando o acesso à lista de mensagens enviadas" na página 80
Ative a restrição de acesso.	"Ativando a restrição para a lista de mensagens enviadas" na página 81

Resultados

Ao concluir essas tarefas, a opção **Correspondências do eMessage** no menu **Campanha** está visível somente para usuários com funções que explicitamente concedem permissão para acessar a lista de correspondências.

Concedendo acesso à lista de mensagens enviadas

Se você restringir o acesso à lista de mensagens enviadas, você deve conceder especificamente o acesso a usuários que devem acessar a lista.

Sobre Esta Tarefa

Os usuários acessam a lista de mensagens enviadas clicando no link **Correspondências do eMessage** no menu **Campanha**. É possível conceder a um usuário acesso à lista de todas as mensagens enviadas designando o usuário uma função administrativa de nível superior que é uma permissão concedida explicitamente para ver o link **Correspondências do eMessage**.

As funções de nível superior padrão incluem **Administrador**, **Executar**, **Projetar** e **Revisar**. As permissões que você concede por meio das funções de nível superior se aplicam a todos os objetos na partição.

Procedimento

1. Acesse `Configurações > Funções e permissões do usuário > Campanha > partição (n)`.
2. Clique em **Salvar e Editar Permissões**. Uma lista de permissões para a partição é aberta. As funções de nível superior disponíveis são listadas na parte superior da página.
3. Na seção **Administração**, conceda explicitamente a permissão **Visualizar página da lista de distribuição** para cada função.

Resultados

Ao ativar restrições de acesso para a lista de mensagens enviadas, os usuários com funções que são concedidas explicitamente a permissão **Visualizar Lista de Página de Mailing** podem ver o link **Correspondências do eMessage** no menu **Campanha**.

O que Fazer Depois

Crie uma função para negar acesso à lista de mensagens enviadas.

Tarefas relacionadas:

"Negando o acesso à lista de mensagens enviadas"

"Ativando a restrição para a lista de mensagens enviadas" na página 81

Negando o acesso à lista de mensagens enviadas

Se você restringir o acesso à lista de mensagens enviadas, você deve negar especificamente o acesso aos usuários que não devem ter permissão para acessar a lista.

Sobre Esta Tarefa

Os usuários acessam a lista de mensagens enviadas clicando no link **Correspondências do eMessage** no menu **Campanha**. É possível impedir que um usuário acesse a lista de todas as mensagens enviadas pela designação do usuário a uma função administrativa de nível superior que é explicitamente negado permissão para ver o link **Correspondências do eMessage**.

As funções de nível superior padrão incluem **Administrador**, **Executar**, **Projetar** e **Revisar**. As permissões que você concede por meio das funções de nível superior se aplicam a todos os objetos na partição. é possível criar novas funções de nível superior para suplementar as funções de nível superior padrão. As novas funções podem conceder ou negar permissões específicas.

Procedimento

1. Acesse **Configurações** > **Funções e permissões do usuário** > **Campanha** > **partição (n)**. A página partição <n> é aberta.
2. Clique em **Incluir função**. Designe um nome à função e insira uma breve descrição. Salve as mudanças e retorne para a página partição <n>.
3. Configure a nova função para negar acesso à lista de correspondências enviadas.
   a. Clique em **Incluir Funções e Designar Permissões**. A página Propriedades para funções administrativas é aberta. A nova função é exibida na lista de funções.
   b. Clique em **Salvar e Editar Permissões**. Uma lista de permissões para a partição é exibida como uma matriz de ícones de seleção que indicam o estado de cada permissão para cada função. A nova função é exibida próxima a outras funções de nível superior na parte superior da matriz.
   c. Na seção **Administração**, negue explicitamente a permissão **Visualizar página de lista de distribuição** para a nova função. Salve as alterações.
4. Designe a nova função aos usuários que deseja impedir de acessar a página de lista de distribuição.
   a. Acesse **Configurações** > **Usuários**. Selecione o usuário que deseja impedir de acessar a lista de mensagens enviadas.
   b. Clique em **Editar funções**. A nova função que você criou na etapa anterior (uma função que é configurada para negar o acesso) aparece na lista de **Funções disponíveis**.
   c. Mova a nova função de **Funções disponíveis** para **Funções**. Salve as alterações.

Resultados

Ao ativar as restrições de acesso para a lista de mensagens enviadas, um usuário que está designado à nova função não pode ver o link **Correspondências do eMessage**.

O que Fazer Depois

Atualize a configuração para ativar restrições de acesso para a lista de mensagens enviadas.

Tarefas relacionadas:

"Concedendo acesso à lista de mensagens enviadas" na página 80

"Ativando a restrição para a lista de mensagens enviadas"

Ativando a restrição para a lista de mensagens enviadas

Os usuários acessam a lista de mensagens enviadas por meio da opção **Correspondências do eMessage** no menu **Campanha**. Se você restringir o acesso à

lista de mensagens enviadas, a propriedade `ID da função de segurança` controla a exibição desta opção de menu e, portanto, controla o acesso à lista de mensagens enviadas.

Sobre Esta Tarefa

Para restringir o acesso à lista de mensagens enviadas, você deve atualizar a propriedade `ID de função de segurança` na configuração do Marketing Platform. Essa propriedade se aplica a todas as partições em sua instalação do Campaign.

Ao preencher o ID da Função de Segurança com o valor correto, a opção **Correspondências do eMessage** está disponível apenas para os usuários com uma função que concede explicitamente a permissão Visualizar Página da Lista de Envio. Os usuários com funções onde a permissão Visualizar Página de Lista de Envio é negada ou não concedida, não é possível ver a opção **Correspondências do eMessage**.

Procedimento

1. Acesse **Configurações** > **Configuração** > **Plataforma** > **Navegação em toda plataforma** > **Menu de navegação principal** > **Campanha** > **Correspondências do eMessage**. Clique em **Correspondências do eMessage** para exibir as definições de configuração.
2. Clicar em **Editar Configurações**.
3. No **ID de função de segurança**, insira `7000`. Salve as alterações.

   Para ver os resultados da mudança na configuração, efetue logout do sistema e efetue login novamente.

Resultados

Apenas usuários com funções que concedem explicitamente a permissão Visualizar Página de Lista de Envio podem ver o link **Correspondências do eMessage** para acessar a lista de mensagens enviadas.

Tarefas relacionadas:

"Concedendo acesso à lista de mensagens enviadas" na página 80

"Negando o acesso à lista de mensagens enviadas" na página 80

Permissões para relatórios do eMessage

Suas permissões do usuário determinam sua capacidade de visualizar relatórios do eMessage.

Para obter informações sobre configurar permissões para acessar relatórios padrão do eMessage, consulte a seção no *IBM EMM Reports Installation and Configuration Guide* para relatório e segurança.

Antes de entrar em contato com o suporte técnico do IBM

Se você encontrar um problema que não puder ser resolvido consultando a documentação, o contato de suporte designado de sua empresa poderá registrar uma chamada com o suporte técnico do IBM. Use essas diretrizes para assegurar que seu problema seja resolvido de modo eficiente e com sucesso.

Se você não for um contato responsável por suporte em sua empresa, entre em contato com seu administrador do IBM para obter informações.

Nota: O Suporte Técnico não grava ou cria scripts da API. Para obter assistência na implementação de nossas ofertas da API, entre em contato com o IBM Professional Services.

Informações para reunir

Antes de entrar em contato com o suporte técnico do IBM, reúna as seguintes informações:

- Uma breve descrição da natureza de seu problema.
- Mensagens de erro detalhadas que são exibidas quando o problema ocorre.
- Etapas detalhadas para reproduzir o problema.
- Arquivos de log, arquivos de sessão, arquivos de configuração e arquivos de dados relacionados.
- Informações de seu produto e ambiente do sistema do , que podem ser obtidas conforme descrito em "Informações do sistema".

Informações do sistema

Ao chamar o suporte técnico do IBM, poderá ser solicitado fornecer informações sobre seu ambiente.

Se o seu problema não impedir que você efetue login, muitas das informações estarão disponíveis na página Sobre, que fornece informações sobre seus aplicativos IBM instalados.

É possível acessar a página Sobre ao selecionar **Ajuda > Sobre**. Se a página Sobre não estiver acessível, verifique um arquivo `version.txt` que está localizado no diretório de instalação de seu aplicativo.

Informações de contato para o suporte técnico do IBM

Para obter maneiras de entrar em contato com o suporte técnico do IBM, consulte o website IBM Product Technical Support: (http://www.ibm.com/support/entry/portal/open_service_request).

Nota: Para inserir uma solicitação de suporte, deve-se efetuar login com uma conta do IBM. Essa conta deverá ser vinculada ao seu número de cliente do IBM. Para saber mais sobre como associar sua conta ao seu número de cliente do IBM, consulte **Recursos de Suporte > Suporte de Software Autorizado** no Portal de Suporte.

Avisos

Essas informações foram desenvolvidas para produtos e serviços oferecidos nos EUA.

A IBM pode não oferecer os produtos, serviços ou recursos discutidos neste documento em outros países. Consulte um representante IBM local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Porém, é responsabilidade do usuário avaliar e verificar a operação de qualquer produto, programa ou serviço não IBM.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desse documento não concede qualquer licença a essas patentes. É possível enviar consultas sobre licença, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Gerência de Relações Comerciais e Industriais da IBM Brasil
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

O parágrafo a seguir não se aplica ao Reino Unido ou a qualquer país no qual tais provisões sejam inconsistentes com a lei local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESSA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO PARA UM PROPÓSITO PARTICULAR. Alguns estados não permitem renúncia de responsabilidade de garantias expressas ou implícitas em certas transações, portanto, essa declaração pode não se aplicar a você.

Essas informações podem incluir imprecisões técnicas ou erros tipográficos. Mudanças são feitas periodicamente nas informações contidas neste documento; essas mudanças serão incorporadas nas novas edições da publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites que não sejam da IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes Web sites. Os materiais contidos nesses Web sites não fazem parte dos materiais para este produto IBM e o uso desses Web sites é de responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados desse programa que desejam ter informações sobre ele para o propósito de ativação de: (i) troca de informações entre programas criados independentemente e outros programas (incluindo esse) e (ii) uso mútuo das informações que foram trocadas, deve entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas aos termos e condições apropriados, incluindo, em alguns casos, pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer outro contrato equivalente.

Quaisquer dados de desempenho contidos neste documento foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros sistemas operacionais podem variar significantemente. Algumas medições podem ter sido feitas em sistemas de nível de desenvolvimento e não há garantia de que essas medições serão as mesmas em sistemas geralmente disponíveis. Além disso, algumas medições podem ter sido estimadas por meio de extrapolação. Resultados reais podem variar. Os usuários desse documento devem verificar os dados aplicáveis para seus ambientes específicos.

Informações quanto a produtos não IBM foram obtidas dos fornecedores desses produtos, seus anúncios publicados ou outras fontes disponíveis publicamente. A IBM não testou esses produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Perguntas sobre as capacidades de produtos não IBM devem ser endereçadas aos fornecedores desses produtos.

Todas as declarações quanto à futura direção ou intenção da IBM estão sujeitas a mudanças ou retiradas sem aviso e representam metas e objetivos apenas.

Todos os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a alteração sem aviso prévio. Preços do revendedor podem variar.

Essas informações contêm exemplos de dados e relatórios usados em operações diárias de negócios. Para ilustrá-las o mais completamente possível, os exemplos incluem os nomes de indivíduos, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer similaridade com nomes e endereços usados por uma empresa real será meramente uma coincidência.

LICENÇA DE COPYRIGHT:

Essas informações contêm programas de aplicativo de amostra no idioma de origem que ilustram técnicas de programação em várias plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de exemplo sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de exemplo são criados. Esses exemplos não foram completamente testados sob todas as condições. A IBM, portanto, não pode garantir ou sugerir a confiabilidade, capacidade de manutenção ou função desses programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de qualquer tipo. A IBM não deve ser responsabilizada por qualquer dano decorrente do uso dos programas de amostra.

Se estiver visualizando essas informações em formato eletrônico, as fotografias e as ilustrações coloridas podem não aparecer.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corp., registradas em muitos países em todo o mundo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas registradas da IBM está disponível na Web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Considerações de Política de Privacidade e Termos de Uso

Produtos de Software IBM, incluindo soluções de software como serviço, ("Ofertas de Software") podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Um cookie é uma parte de dados que um website pode enviar para o seu navegador, que pode, então, ser armazenada em seu computador como uma tag que identifica o seu computador. Em muitos casos, nenhuma informação pessoal é coletada por esses cookies. Se uma Oferta de Software que você estiver usando permitir que você colete informações pessoais por meio de cookies e tecnologias similares, nós o informamos sobre os aspectos específicos abaixo.

Dependendo das configurações implementadas, esta Oferta de Software pode usar cookies de sessão e persistentes que coletam o nome de usuário de cada usuário e outras informações pessoais com propósitos de gerenciamento de sessão, usabilidade de usuário aprimorada ou outros propósitos de rastreio de uso ou funcionais. Esses cookies podem ser desativados, mas sua desativação também eliminará a funcionalidade que eles ativam.

Várias jurisdições regulamentam a coleta de informações pessoais por meio de cookies e tecnologias similares. Se as configurações implementadas para essa Oferta de Software fornecerem a você, como Cliente, a capacidade de coletar informações pessoais de usuários finais por meio de cookies e outras tecnologias, você deve buscar seu próprio conselho jurídico sobre quaisquer leis aplicáveis a tal coleta de dados, incluindo quaisquer requisitos para fornecer aviso e consentimento onde apropriado.

A IBM requer que os Clientes (1) forneçam um link claro e evidente para os termos de uso do website do Cliente (por exemplo, política de privacidade) que inclui um link para a coleção de dados da IBM e do Cliente e práticas de uso (2) notifiquem que cookies e indicadores de gifs/web claros estão sendo colocados no computador do visitante pela IBM em nome do Cliente juntamente com uma explicação do propósito de tal tecnologia e (3) no alcance exigido por lei, obtenham consentimento dos visitantes do website antes da colocação de cookies e indicadores de gifs/web claros colocados pelo Cliente ou IBM em nome do cliente nos dispositivos do visitante do website

Para obter informações adicionais sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Declaração de Privacidade Online da IBM em http://www.ibm.com/privacy/details/us/en na seção intitulada "Cookies, indicadores da web e outras tecnologias."